Lucas sequences whose 8th term is a square

A. Bremner* N. Tzanakis†

February 1, 2008

1 Abstract

Let P and Q be non-zero integers. The Lucas sequence $\{U_n(P,Q)\}$ is defined by

$$U_0 = 0, \quad U_1 = 1, \quad U_n = PU_{n-1} - QU_{n-2} \quad (n \geq 2).$$

For each positive integer $n \leq 7$ we describe all Lucas sequences with $(P,Q) = 1$ having the property that $U_n(P,Q)$ is a perfect square. The arguments are elementary. We also find all Lucas sequences such that $U_8(P,Q)$ is a perfect square. This reduces to a number of problems of similar type, namely, finding all points on an elliptic curve defined over a quartic number field subject to a "$\mathbf{Q}$-rationality" condition on the X-coordinate. This is achieved by p-adic computations (for a suitable prime p) using the formal group of the elliptic curve.

2 Introduction

Let P and Q be non-zero integers. The Lucas sequence $\{U_n(P,Q)\}$ is defined by

$$U_0 = 0, \quad U_1 = 1, \quad U_n = PU_{n-1} - QU_{n-2} \quad (n \geq 2). \tag{1}$$

The sequence $\{U_n(1,-1)\}$ is the familiar Fibonacci sequence, and it was proved by Cohn [11] in 1964 that the only perfect square greater than 1 in this sequence is $U_{12} = 144$. The question arises, for which parameters P, Q, can $U_n(P,Q)$ be a perfect square? In what follows, we shall assume that we are not dealing with the degenerate sequences corresponding to $(P,Q) = (\pm 1, 1)$, where U_n is periodic with period 3, and we also assume $(P,Q) \neq (-2,1)$ (in which case $U_n = \square$ precisely when n is an odd square) and $(P,Q) \neq (2,1)$ (when $U_n = \square$ precisely

*Department of Mathematics, Arizona State University, Tempe AZ, USA, e-mail: bremner@asu.edu, http://˜andrew/bremner.html

†Department of Mathematics, University of Crete, Iraklion, Greece, e-mail: tzanakis@math.uoc.gr , http://www.math.uoc.gr/˜tzanakis

when n is square). Ribenboim and McDaniel [15] with only elementary methods show that when P and Q are *odd*, and $P^2 - 4Q > 0$, then U_n can be square only for $n = 0, 1, 2, 3, 6$ or 12; and that there are at most two indices greater than 1 for which U_n can be square. They characterize fully the instances when $U_n = \square$, for $n = 2, 3, 6$. Bremner & Tzanakis [1] extend these results by determining all Lucas sequences $\{U_n(P, Q)\}$ with $U_{12} = \square$, subject only to the restriction that $\gcd(P, Q) = 1$ (it turns out that the Fibonacci sequence provides the only example). Under the same hypothesis, all Lucas sequences with $\{U_n(P, Q)\}$ with $U_9 = \square$ are determined. There seems little mention in the literature of when under general hypotheses $U_n(P, Q)$ can be a perfect square. Note that for $n \geq 1$, $U_n(kP, k^2Q) = k^{n-1}U_n(P, Q)$, and so for fixed P, Q, and *even* n, appropriate choice of k gives a sequence with $U_n(kP, k^2Q)$ a perfect square. The restriction to $(P, Q) = 1$ is therefore a sensible one, and we shall assume this from now on. A small computer search reveals sequences with $U_n(P, Q)$ a perfect square, only for $n = 0, \ldots, 8$, and $n = 12$. Bremner & Tzanakis [1] have addressed the case $n = 12$. Section 3 of this paper addresses the case of $U_n(P, Q) = \square,\ n \leq 7$, which can be treated entirely elementarily. The remainder of the paper (section 4) addresses the case $U_8(P, Q) = \square$. This reduces to a number of problems of similar type, namely, finding all points on an elliptic curve defined over a number field K subject to a "$\mathbb{Q}$-rationality" condition on the X-coordinate. The elliptic curves we consider have K-rank at most 2, with degree $[K : \mathbb{Q}] = 4$, and so this problem is of "Chabauty" type in the language of Nils Bruin. Bruin has powerful techniques for addressing this type of problem, and [5], [6], [7], [8] provide details and examples. We persevere in writing the current paper to describe in very concrete form the underlying mathematics, based on the work of Flynn and Wetherell [13], together with a theorem that is essentially due to Th. Skolem from the 1930s to deal with the example of our rank 2 elliptic curve. The latest release of Magma now contains Bruin's routines for much of the calculations of this paper, but we feel it is still worthwhile to give some (minimal) details of the computations, in order to expose the underlying theory and make it accessible to the reader, as well as for those without access to Magma.

3 Solution of $U_n(P, Q) = \square,\ n \leq 7$

Certainly $U_2(P, Q) = \square$ if and only if $P = a^2$, and $U_3(P, Q) = \square$ if and only if $P^2 - Q = a^2$.

Now $U_4(P, Q) = \square$ if and only if $P(P^2 - 2Q) = \square$, so if and only if either $P = \delta a^2, Q = \frac{1}{2}(a^4 - \delta b^2)$, or $P = 2\delta a^2, Q = 2a^4 - \delta b^2$, with $\delta = \pm 1$ (where, in the first instance, ab is odd and in the second instance b is odd).

The demand that $U_5(P, Q)$ be square is that $P^4 - 3P^2Q + Q^2 = \square$, equivalently, that $1 - 3x + x^2 = \square$, where $x = Q/P^2$. Parametrizing the quadric, $Q/P^2 = (5\lambda^2 + 6\lambda\mu + \mu^2)/(4\lambda\mu)$, where, without loss of generality, $(\lambda, \mu) = 1$,

$\lambda > 0$, and $\mu \not\equiv 0 \pmod 5$. Necessarily $(\lambda, \mu) = (a^2, \pm b^2)$, giving $(P, Q) = (2ab, 5a^4 + 6a^2b^2 + b^4)$ or $(2ab, -5a^4 + 6a^2b^2 - b^4)$ if a and b are of opposite parity, and $(P, Q) = (ab, \frac{1}{4}(5a^4 + 6a^2b^2 + b^4))$ or $(ab, \frac{1}{4}(-5a^4 + 6a^2b^2 - b^4))$, if a and b are both odd.
The demand that $U_6(P, Q)$ be square is that $P(P^2 - Q)(P^2 - 3Q) = \square$, which leads to one of seven cases: $P = a^2$, $P^2 - Q = b^2$, with $-2a^4 + 3b^2 = \square$; $P = a^2$, $P^2 - Q = -2b^2$, with $a^4 + 3b^2 = \square$; $P = -a^2$, $P^2 - Q = 2b^2$, with $a^4 - 3b^2 = \square$; and $P = 3a^2$, $P^2 - Q = \delta b^2$, $(\delta = \pm 1, \pm 2)$, with $-\frac{6}{\delta}a^4 + b^2 = \square$. So finitely many parametrizations result (which can easily be obtained, if we wish to do so).
The demand that $U_7(P, Q)$ be square is that $P^6 - 5P^4Q + 6P^2Q^2 - Q^3 = \square$, equivalently, that $1 + 5x + 6x^2 + x^3 = y^2$, where $x = -Q/P^2$. This latter elliptic curve has rank 1, with generator $P_0 = (-1, 1)$, and trivial torsion. Accordingly, sequences with $U_7(P, Q) = \square$ are parametrized by the multiples of P_0 on the above elliptic curve, corresponding to $(\pm P, Q) = (1, 1)$, $(1, 5)$, $(2, -1)$, $(5, 21)$, $(1, -104)$, $(21, 545)$, $(52, 415)$,...

4 Solution of $U_8(P, Q) = \square$

The remainder of the paper will be devoted to the proof of the following result:

Theorem. *The only non-degenerate sequences where* $(P, Q) = 1$ *and* $U_8(P, Q) = \square$ *are given by* $U_8(1, -4) = 21^2$ *and* $U_8(4, -17) = 620^2$.

4.1 The auxiliary equations

The demand that $U_8(P, Q)$ be square is that $P(P^2 - 2Q)(P^4 - 4P^2Q + 2Q^2) = \square$.

4.1.1 P odd

It follows that $(P, P^2 - 2Q, P^4 - 4P^2Q + 2Q^2) = (a^2, b^2, c^2)$, $(a^2, -b^2, -c^2)$, $(-a^2, b^2, -c^2)$, or $(-a^2, -b^2, c^2)$, where a, b, c are positive integers with ab odd. The latter two possibilities are impossible modulo 4, and the first two possibilities lead respectively to:

$$-a^8 + 2a^4b^2 + b^4 = 2c^2 \quad (2)$$
$$-a^8 - 2a^4b^2 + b^4 = -2c^2 \quad (3)$$

Equation (2) is related to the elliptic curves $\mathcal{E}_1$ and $\mathcal{E}_2$ (see (8) and (10), respectively) and equation (3) is related to the elliptic curves $\mathcal{E}_3$ and $\mathcal{E}_4$ (see (13) and (15), respectively). According to Proposition 1 the only positive solutions to the above equations are $(a, b) = (1, 1), (1, 3)$ and $(1, 1)$ respectively, leading to $(P, Q) = (1, 0), (1, -4)$ and $(1, 1)$, from which we reject the first one. The last gives a degenerate sequence.

4.1.2 P even

Now Q is odd, and 2 exactly divides both $P^4-4P^2Q+2Q^2$ and P^2-2Q, forcing $P \equiv 0 \pmod 4$. Put $P=4p$, so that $U_8=\square$ if and only if $p(8p^2-Q)(128p^4-32p^2Q+Q^2)=\square$, with $(p,Q)=1$. It follows that $(p, 8p^2-Q, 128p^4-32p^2Q+Q^2) = (a^2,b^2,c^2)$, $(a^2,-b^2,-c^2)$, $(-a^2,b^2,-c^2)$, or $(-a^2,-b^2,c^2)$, where a, b, c are positive integers, $(a,b)=1$ and bc is odd. The middle two possibilities are impossible modulo 4, and the remaining two possibilities lead respectively to:

$$-64a^8+16a^4b^2+b^4 = c^2 \quad (4)$$

$$-64a^8-16a^4b^2+b^4 = c^2 \quad (5)$$

Equation (4) is related to the elliptic curves $\mathcal{E}_5, \mathcal{E}_6, \mathcal{E}_7$ and $\mathcal{E}_8$ (see (18), (20), (22) and (24), respectively). According to Proposition 1 the only positive solution which leads to a desired pair (P,Q) is $(a,b)=(1,5)$, leading to $(P,Q)=(4,-17)$. Equation (5) is related to the elliptic curves $\mathcal{E}_9, \mathcal{E}_{10}, \mathcal{E}_{11}$ and $\mathcal{E}_{12}$ (see (27), (29), (33) and (35), respectively). According to Proposition 1, which deals with $\mathcal{E}_i$ with $i=9,11,12$ and Proposition 4, which deals with $\mathcal{E}_{10}$, there are no positive solutions (a,b).

4.2 The elliptic curves

In this section we reduce the solution of equations (2)-(5) to the solution of a number of problems all of which fit the following general shape:

Problem 1. *Let*

$$\mathcal{E} \,:\, Y^2+a_1XY+a_3Y = X^3+a_2X^2+a_4X+a_6 \quad (6)$$

be an elliptic curve defined over $\mathbb{Q}(\alpha)$, where α is a root of a polynomial $f(X) \in \mathbb{Z}[X]$, irreducible over $\mathbb{Q}$, of degree $d \geq 2$, and let $\beta, \gamma \in \mathbb{Q}(\alpha)$ be algebraic integers. Find all points $(X,Y) \in \mathcal{E}(\mathbb{Q}(\alpha))$ for which $\beta X+\gamma$ is a rational number.

We shall see that equations (2)-(5) lead to elliptic curves $\mathcal{E}_i$, $i=1,\ldots,12$, and so 12 instances of Problem 1; in each case we specify the corresponding "condition on X-coordinate" $\beta X+\gamma \in \mathbb{Q}$. In all but one case the elliptic curves have rank 1 and in the exceptional case the rank is 2.
We need details of two number fields. First, let θ be a root of $f_1(x)=x^4+2x^2-1$, with $K_1=\mathbb{Q}(\theta)$. The class number of K_1 is 1, the maximal order $\mathcal{O}_1$ of K_1 is $\mathbb{Z}[\theta]$, and fundamental units of $\mathcal{O}_1$ are $\eta_1=\theta$, $\eta_2=2-3\theta+\theta^2-\theta^3$. The factorization of 2 is $2=\eta_1^{-4}\eta_2^2(1+\theta)^4$.
Second, let ϕ be a root of $f_2(x)=x^4+4x^2-4$, with $K_2=\mathbb{Q}(\phi)$. The class number of K_2 is 1, the maximal order $\mathcal{O}_2$ is $\mathbb{Z}[1,\phi,\frac{1}{2}\phi^2,\frac{1}{2}\phi+\frac{1}{4}\phi^3]$, and fundamental units are $\epsilon_1=\frac{1}{2}\phi+\frac{1}{4}\phi^3$, $\epsilon_2=2+2\phi+\frac{1}{2}\phi^2+\frac{1}{2}\phi^3$. The factorization of 2 is $2=\epsilon_2^{-2}\pi^4$, where $\pi=1+\frac{3}{2}\phi+\frac{1}{4}\phi^3$.

4.2.1 Equation (2) and curves $\mathcal{E}_1, \mathcal{E}_2$

The factorization of (2) over K_1 is

$$(b - \theta a^2)(b + \theta a^2)(b^2 + (2 + \theta^2)a^4) = 2\Box,$$

and it is easy to see that the gcd of any two (ideal) terms on the left hand side is equal to $(1 + \theta)$, with the last term exactly divisible by $(1 + \theta)^2$. Hence,

$$(b + \theta a^2)(b^2 + (2 + \theta^2)a^4) = \pm\eta_1^i \eta_2^j (1 + \theta)\Box,$$

where $i, j = 0, 1$. Specializing θ at the real root 0.643594... of $f_1(x)$, and using $b > 0$, then necessarily the sign on the right hand side must be positive. By putting $b/a^2 = \delta^{-1}x/(1 + \theta)$, where $\delta = \eta_1^i \eta_2^j$, our problem reduces to finding all K_1-points (x, y) on the curves

$$(x + \theta(1 + \theta)\delta)(x^2 + (2 + \theta^2)(1 + \theta)^2\delta^2) = y^2,$$

subject to $\delta^{-1}x/(1 + \theta) \in \mathbb{Q}$, with $\delta = 1$, η_1, η_2, or $\eta_1\eta_2$. Putting

$$(x, y) = (2X - (\theta + \theta^2)\delta, 2(1 + \theta^2)Y)$$

gives

$$Y^2 = X(X^2 - (\theta + \theta^2)\delta X + (1 + \theta + \theta^3)\delta^2); \tag{7}$$

and the condition on the X-coordinate becomes:

$$-\theta + \frac{(3 - 3\theta + \theta^2 - \theta^3)X}{\delta} \in \mathbb{Q}.$$

There are several computer packages now available for computing with elliptic curves E over number fields K. We mention Algae [3] for KASH and m-Algae [4] for MAGMA, both by Nils Bruin; the TECC [14] calculator of Kida, also for KASH; and Simon's package [22] for Pari-GP. They are extremely useful in computing ranks, and generators for the group $E(K)/2E(K)$. In each case below, it turns out that the points generating $E(K)$ modulo $2E(K)$ are actually generators for the group $E(K)$ itself. This was proved using detailed height calculations over the appropriate number field, with careful estimates for the difference $\hat{h}(Q) - \frac{1}{2}h(Q)$ where $\hat{h}(Q)$ is the canonical height of the point Q, and $h(Q)$ the logarithmic height. The standard Silverman bounds [20] are numerically too crude for our purposes, so recourse was made to the refinements of Siksek [18]. Full details of the argument are given in an appendix to this paper [2].
For the curve (7) under immediate consideration, the cases $\delta = \eta_1, \eta_1\eta_2$, give rise to curves of rank 0, and $\delta = 1$, η_2, to curves of rank 1.
First, the curve (7) at $\delta = 1$ is

$$\mathcal{E}_1 : Y^2 = X(X^2 - (\theta + \theta^2)X + (1 + \theta + \theta^3)) \tag{8}$$

possessing only 2-torsion over K_1, and with generator

$$G_1 = (\frac{3+4\theta+\theta^2}{2},\ \frac{-4-6\theta-\theta^2-5\theta^3}{2}). \tag{9}$$

The condition on the X-coordinate is

$$-\theta + (3-3\theta+\theta^2-\theta^3)X \in \mathbb{Q}.$$

The point (9) returns $(a,b) = (1,3)$.

Second, the curve at $\delta = \eta_2$ is

$$\mathcal{E}_2 : Y^2 = X(X^2 - (\theta-\theta^2)X + (1-\theta-\theta^3)) \tag{10}$$

possessing only 2-torsion over K_1, with generator

$$G_2 = (\frac{1-\theta^2}{2},\ \frac{1-\theta}{2}). \tag{11}$$

The condition on the X-coordinate is

$$-\theta + (3+3\theta+\theta^2+\theta^3)X \in \mathbb{Q}.$$

The point (11) returns $(a,b) = (1,1)$.

Both curves (8) and (10) are minimal models.

4.2.2 Equation (3) and curves $\mathcal{E}_3, \mathcal{E}_4$

As above, (3) leads to an equation

$$(b + \frac{1}{\theta}a^2)(b^2 + (-2+\frac{1}{\theta^2})a^4) = \pm\eta_1^i\eta_2^j(1+\theta)\square,$$

where $i,j = 0,1$. Specializing at the positive real root 0.643594... of $f_1(x)$, the sign of the right hand side must be positive. Putting $b/a^2 = \delta^{-1}x/(1+\theta)$, where $\delta = \eta_1^i\eta_2^j$, we thus have to find all K_1-points (x,y) on the curves

$$(x + \frac{1+\theta}{\theta}\delta)(x^2 + (-2+\frac{1}{\theta^2})(1+\theta)^2\delta^2) = y^2,$$

such that $\delta^{-1}\frac{x}{1+\theta} \in \mathbb{Q}$, for $\delta = 1$, η_1, η_2, or $\eta_1\eta_2$.
Now put

$$(x,y) = (2X - \frac{1+\theta}{\theta}\delta,\ 2(1+\theta^2)Y),$$

to give

$$Y^2 = X(X^2 + (-1-2\theta-\theta^3)\delta X + (1+\theta+\theta^3)\delta^2); \tag{12}$$

and the condition on the X-coordinate is

$$\frac{2}{1+\theta}\frac{X}{\delta} - \frac{1}{\theta} \in \mathbb{Q}.$$

The cases $\delta = 1, \eta_2$ give curves of rank 0; the remaining two cases are of rank 1. First, the curve (12) at $\delta = \eta_1$ is

$$\mathcal{E}_3 : Y^2 = X(X^2 + (-1-\theta)X + (\theta + \theta^2 - \theta^3)), \tag{13}$$

possessing only 2-torsion over K_1, with generator

$$G_3 = (\frac{1-\theta^2}{2},\ \frac{\theta^2+\theta^3}{2}). \tag{14}$$

The condition on the X-coordinate is

$$-2\theta - \theta^3 + (-3 + 7\theta - \theta^2 + 3\theta^3)X \in \mathbb{Q}.$$

The point (14) returns $(a, b) = (1, 1)$.

Second, the curve (12) at $\delta = \eta_1\eta_2$ is

$$\mathcal{E}_4 : Y^2 = X(X^2 + (-1+\theta)X + (-\theta + \theta^2 + \theta^3)), \tag{15}$$

a conjugate of the curve (13) under $\theta \to -\theta$. Its generator is therefore

$$G_4 = (\frac{1-\theta^2}{2},\ \frac{\theta^2-\theta^3}{2}). \tag{16}$$

The condition on the X-coordinate is

$$-2\theta - \theta^3 + (3 + 7\theta + \theta^2 + 3\theta^3)X \in \mathbb{Q}.$$

The point (16) again returns $(a, b) = (1, 1)$.

4.2.3 Equation (4) and curves $\mathcal{E}_i, i = 5, \ldots, 8$

As above, (4) leads to an equation of type

$$(b + 2\phi a^2)(b^2 + 4(4+\phi^2)a^4) = \pm\epsilon_1^i\epsilon_2^j\Box,$$

for $i, j = 0, 1$. Specializing ϕ at the positive real root 0.910179... of $f_2(x)$, it follows that the sign must be positive. For $a \neq 0$, put $b/a^2 = \delta^{-1}x$, where $\delta = \epsilon_1^i\epsilon_2^j$, which leads to seeking all K_2-points (x, y) on the curves

$$(x + 2\phi\delta)(x^2 + 4(4+\phi^2)\delta^2) = y^2,$$

subject to $\delta^{-1}x \in \mathbb{Q}$, with $\delta = 1$, ϵ_1, ϵ_2, or $\epsilon_1\epsilon_2$, that is, $\delta = 1$, $\frac{1}{2}\phi + \frac{1}{4}\phi^3$, $2 + 2\phi + \frac{1}{2}\phi^2 + \frac{1}{2}\phi^3$, $1 + \frac{3}{2}\phi + \frac{1}{2}\phi^2 + \frac{1}{4}\phi^3$. Put

$$(x, y) = (4X - 2\phi\delta,\ (2 + \phi^2)^2 Y)$$

to give

$$Y^2 = X(X^2 - \phi\delta X + (1 + \frac{1}{2}\phi^2)\delta^2), \tag{17}$$

where the condition on X-coordinate has become

$$-2\phi + \frac{4}{\delta}X \in \mathbb{Q}.$$

All four curves are of rank 1. The curve (17) with $\delta = 1$ has equation

$$\mathcal{E}_5 : Y^2 = X(X^2 - \phi X + (1 + \frac{1}{2}\phi^2)), \tag{18}$$

possessing only 2-torsion over K_2, with generator

$$G_5 = (2 - 2\phi + \frac{1}{2}\phi^2 - \frac{1}{2}\phi^3,\ 5 - 5\phi + \phi^2 - \phi^3). \tag{19}$$

The condition on the X-coordinate is

$$-2\phi + 4X \in \mathbb{Q}.$$

Twice the generator at (19) is the point

$$(X, Y) = (\frac{5}{4} + \frac{1}{2}\phi, \frac{1}{2} + \frac{7}{4}\phi - \frac{3}{16}\phi^2 + \frac{5}{16}\phi^3),$$

which leads to $(a, b) = (1, 5)$.

The curve (17) with $\delta = \epsilon_1$ has equation

$$\mathcal{E}_6 : Y^2 = X(X^2 + (-1 + \frac{1}{2}\phi^2)X + (1 - \frac{1}{2}\phi^2)), \tag{20}$$

possessing only 2-torsion over K_2, with generator

$$G_6 = (1 - \frac{1}{2}\phi^2,\ 1 - \frac{1}{2}\phi^2). \tag{21}$$

The condition on the X-coordinate is

$$-2\phi + (6 + \phi^3)X \in \mathbb{Q}.$$

The curve (17) with $\delta = \epsilon_2$ has equation

$$\mathcal{E}_7 : Y^2 = X(X^2 + (-2 - 2\phi - \frac{1}{2}\phi^3)X + (13 + 14\phi + \frac{5}{2}\phi^2 + 3\phi^3)), \tag{22}$$

possessing only 2-torsion over K_2, with generator

$$G_7 = (1 + \frac{1}{2}\phi + \frac{1}{4}\phi^3,\ -3 - 3\phi - \frac{1}{2}\phi^2 - \frac{1}{2}\phi^3). \tag{23}$$

The condition on X-coordinate has become

$$-2\phi + 2(4 - 4\phi + \phi^2 - \phi^3)X \in \mathbb{Q}.$$

The curve (17) with $\delta = \epsilon_1\epsilon_2$ has equation

$$\mathcal{E}_8 : Y^2 = X(X^2 + (-1 - \phi - \frac{1}{2}\phi^2 - \frac{1}{2}\phi^3)X + (5 + 6\phi + \frac{3}{2}\phi^2 + \phi^3)), \tag{24}$$

possessing only 2-torsion over K_2, with generator

$$G_8 = (1 + \frac{1}{2}\phi + \frac{1}{4}\phi^3,\ -2 - 2\phi - \frac{1}{2}\phi^3). \tag{25}$$

The condition on X-coordinate has become

$$-2\phi + (-12 + 14\phi - 2\phi^2 + 3\phi^3)X \in \mathbb{Q}.$$

All curves are minimal models.

4.2.4 Equation (5) and curves $\mathcal{E}_i, i = 9, \ldots, 12$

As in the third case, we deduce an equation in $\mathcal{O}_2$:

$$(b + \frac{4}{\phi}a^2)(b^2 + (-16 + \frac{16}{\phi^2})a^4) = \pm\epsilon_1^i\epsilon_2^j\Box,$$

where $i, j = 0, 1$, and specializing at the positive real root of $f_2(x)$, the sign must be positive. For $a \neq 0$, put $b/a^2 = \delta^{-1}x$, where $\delta = \epsilon_1^i\epsilon_2^j$. This leads to finding all K_2-points (x, y) on the curves

$$(x + \frac{4}{\phi}\delta)(x^2 + (-16 + \frac{16}{\phi^2})\delta^2) = \Box,$$

with $\delta^{-1}x \in \mathbb{Q}$, and $\delta = 1$, ϵ_1, ϵ_2, $\epsilon_1\epsilon_2$. Putting

$$(x, y) = (4X - \frac{4}{\phi}\delta,\ (2 + \phi^2)^2 Y)$$

gives

$$Y^2 = X(X^2 - \frac{2}{\phi}\delta X + (-1 + \frac{2}{\phi^2})\delta^2), \tag{26}$$

and the condition on X becomes

$$-\frac{4}{\phi} + \frac{4}{\delta}X \in \mathbb{Q}.$$

The curve (26) with $\delta = 1$ has equation

$$\mathcal{E}_9 : Y^2 = X(X^2 + (-2\phi - \frac{1}{2}\phi^3)X + (1 + \frac{1}{2}\phi^2)), \tag{27}$$

of rank 1, possessing only 2-torsion over K_2, with generator

$$G_9 = (1 + \frac{1}{2}\phi + \frac{1}{4}\phi^3, -\phi). \tag{28}$$

of canonical height 0.125726743336419... The condition on X has become

$$-4\phi - \phi^3 + 4X \in \mathbb{Q}.$$

The curve (26) with $\delta = \epsilon_1$ has equation

$$\mathcal{E}_{10} : Y^2 = X(X^2 + (-1 - \frac{1}{2}\phi^2)X + (1 - \frac{1}{2}\phi^2)), \tag{29}$$

and is of rank 2, possessing only 2-torsion over K_2, with generators

$$P_1 : (X, Y) = (1, \frac{1}{2}\phi^2), \tag{30}$$

and

$$P_2 : (X, Y) = (\frac{1}{2}\phi + \frac{1}{2}\phi^2 - \frac{1}{4}\phi^3, 1 - \frac{3}{2}\phi^2). \tag{31}$$

The condition on X is

$$-4\phi - \phi^3 + (6\phi + \phi^3)X \in \mathbb{Q} \tag{32}$$

The curve (26) with $\delta = \epsilon_2$ has equation

$$\mathcal{E}_{11} : Y^2 = X(X^2 + (-4 - 5\phi - \phi^2 - \phi^3)X + (13 + 14\phi + \frac{5}{2}\phi^2 + 3\phi^3)), \tag{33}$$

of rank 1, possessing only 2-torsion over K_2, with generator

$$G_{11} = (2 + 2\phi + \frac{1}{2}\phi^2 + \frac{1}{2}\phi^3, -2 - 2\phi - \frac{1}{2}\phi^2 - \frac{1}{2}\phi^3). \tag{34}$$

The condition on X becomes

$$-4\phi - \phi^3 + (8 - 8\phi + 2\phi^2 - 2\phi^3)X \in \mathbb{Q}.$$

The curve (26) with $\delta = \epsilon_1\epsilon_2$ has equation

$$\mathcal{E}_{12} : Y^2 = X(X^2 + (-3 - 3\phi - \frac{1}{2}\phi^2 - \frac{1}{2}\phi^3)X + (5 + 6\phi + \frac{3}{2}\phi^2 + \phi^3)), \tag{35}$$

of rank 1, possessing only 2-torsion over K_2, with generator

$$G_{12} = (1 + \frac{1}{2}\phi + \frac{1}{4}\phi^3, -1 - \phi - \frac{1}{2}\phi^2 - \frac{1}{2}\phi^3). \tag{36}$$

The condition on X has become

$$-4\phi - \phi^3 + (-12 + 14\phi - 2\phi^2 + 3\phi^3)X \in \mathbb{Q}.$$

All curves are minimal models.

4.3 Cases corresponding to rank 1 elliptic curves

We gave a detailed discussion of the solution of Problem 1 for rank one elliptic curves in section 4 of our companion paper [1], in which we also gave a number of concrete examples. Therefore, we confine ourselves here in giving all necessary data for the corresponding rank one elliptic curves of section 4.2 and saying that, following exactly the same method and working p-adically with $p = 3$, we conclude the following result:

Proposition 1. *For each elliptic curve $\mathcal{E}_i$, $i = 1, \ldots, 9$, and $i = 11, 12$, the only points on $\mathcal{E}_i$ whose X-coordinate belongs to the appropriate quartic field and which satisfies the corresponding condition $\beta X + \gamma \in \mathbb{Q}$, are given by the following:*

- *Elliptic curve $\mathcal{E}_1$: points $\pm G_1$, giving $a = \pm 1, b = 3$ at (2).*
  From section 4.1.1, $P = 1, Q = -4$.
- *Elliptic curve $\mathcal{E}_2$: points $\pm G_2$, giving $a = \pm 1, b = 1$ at (2).*
  From section 4.1.1, $P = 1, Q = 1$.
- *Elliptic curve $\mathcal{E}_3$: points $\pm G_3$, giving $a = \pm 1, b = -1$ at (3).*
  From section 4.1.1, $P = 1, Q = 1$.
- *Elliptic curve $\mathcal{E}_4$: points $\pm G_4$, giving $a = \pm 1, b = 1$ at (3).*
  From section 4.1.1, $P = 1, Q = 1$.
- *Elliptic curve $\mathcal{E}_5$: points $\pm 2G_5$, giving $a = \pm 1, b = 5$ at (4).*
  From section 4.1.2, $P = 4, Q = -17$.
- *Elliptic curve $\mathcal{E}_6$: no point.*
- *Elliptic curve $\mathcal{E}_7$: points $\pm 2G_7$, giving $a = \pm 1, b = 2$ at (4).*
  From section 4.1.2, $P = 4, Q = 4$, rejected (we assumed P, Q relatively prime).

- *Elliptic curve* $\mathcal{E}_8$: *points* $\pm 2G_8$, *giving* $a = \pm 1, b = 0$ *at (4), which is impossible.*

- *Elliptic curves* $\mathcal{E}_9, \mathcal{E}_{11}, \mathcal{E}_{12}$: *no points.*

4.4 Cases corresponding to rank 2 elliptic curves

For the solution of Problem 1 when the rank of the elliptic curve is 2, we make the following assumptions:

Assumption 1. There exists a rational prime p with the following properties:

- $f(X)$ is irreducible in $\mathbb{Q}_p[X]$. This implies that p is a prime divisor of the number field $\mathbb{Q}(\alpha)$ and there is only one discrete (normalized) valuation v defined on $\mathbb{Q}(\alpha)$ with $v(p) = 1$. Moreover, the completion of $\mathbb{Q}(\alpha)$ with respect to v is $\mathbb{Q}_p(\alpha)$ and, according to our assumptions, $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = d$.

- The coefficients of (6) are in $\mathbb{Z}_p[\alpha]$.

- Equation (6) is a minimal Weierstrass equation for $\mathcal{E}/\mathbb{Q}_p(\alpha)$ at v.

- $\beta, \gamma \in \mathbb{Q}_p(\alpha)$ are p-adic units.

Assumption 2. We know two independent points $Q_1, Q_2 \in \mathcal{E}(\mathbb{Q}(\alpha))$, each having the form $(s/t^2, u/t^3)$ with $s, u \in \mathbb{Z}[\alpha]$, t a positive integer divisible by p and $(\mathrm{Norm}(s), t) = (\mathrm{Norm}(u), t) = 1$; here Norm denotes norm relative to the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$. If $p = 2$ we assume something more, namely, that t is divisible by $p^2 = 4$.

According to the notation and facts in section 4 of our paper [1], $Q_i \in \hat{\mathcal{E}}(\mathcal{M}^r)$, $(i = 1, 2)$. The same arguments used therein, lead to the following conclusion:

Fact 2. *Let* $P = (X_0, Y_0)$ *be any finite point of* $\mathcal{E}(\mathbb{Q})$ *and let* n_1, n_2 *denote integer variables. Then, both* $\beta x(P + n_1 Q_1 + n_2 Q_2) + \gamma$ *and* $(\beta x(n_1 Q_1 + n_2 Q_2) + \gamma)^{-1}$ *can be expressed as* $\theta_0(n_1, n_2) + \theta_1(n_1, n_2)\alpha + \cdots + \theta_{d-1}(n_1, n_2)\alpha^{d-1}$, *where each* $\theta_i(n_1, n_2)$ *is a p-adically convergent power series in* n_1, n_2 *with coefficients in* $\mathbb{Z}_p$, *having also the following property: For every* $(k, \ell) \neq (0, 0)$,

$$v(\textit{coefficient of } n_1^k n_2^\ell) \geq \begin{cases} \left\lfloor \frac{(p-2)(k+\ell)}{p-1} \right\rfloor + 1 & \textit{if } p \geq 3 \\ k + \ell + 1 & \textit{if } p = 2 \end{cases} . \tag{37}$$

The coefficients of the series θ_i depend on the coordinates of Q_1, Q_2 and, in case of $\beta x(P + n_1 Q_1 + n_2 Q_2) + \gamma$, also on the coordinates of P.

Assumption 3. The typical point on $\mathcal{E}(\mathbb{Q}(\alpha))$ can be expressed in the form $P + n_1Q_1 + n_2Q_2$, where P is chosen from a finite explicitly known set of points, including the zero point.

Under Assumptions 1-3, problem 1 is clearly reduced to solving the system of equations $\theta_1(n_1, n_2) = 0, \ldots, \theta_{d-1}(n_1, n_2) = 0$ for each value of P. In [1] we had a similar problem, but for a curve of rank 1, and the system of equations we had to solve was in one unknown n_1. In that situation, Strassman's theorem (see, for example, Theorem 4.1 in [1]) was applicable, but not in the present one, where we have two unknowns n_1, n_2. Instead, we apply a theorem, which we state and prove below, inspired by the paper of Th. Skolem [23].

It is worth mentioning that, in a similar situation, S. Duquesne in [12] applied a different method based on his explicit version of a p-adic Weierstrass preparation theorem of T. Sugatani [25] (see sections 2 and 3 of [12]). That explicit version of Sugatani's theorem is interesting, but from our experience (in a first unpublished version of this paper, we employed Duquesne's method) its application is more complicated.

Our remarks a few lines above make evident that, in order to solve problem 1, we must know how to find explicitly all p-adic integer solutions of a system of equations $F_1 = 0, F_2 = 0$, for appropriate series $F_1, F_2 \in \mathbb{Z}_p[[x_1, x_2]]$. In a more general setting we state and prove the theorem below which we will apply in the special case of two unknowns.

Theorem 3. *Let p be a prime and for $r = 1, \ldots, n$ let*

$$F_r(x_1, \ldots, x_n) = \sum_{i=0}^{\infty} p^i f_{ir}(x_1, \ldots, x_n) \, ,$$

where $f_{ir} \in \mathbb{Z}_p[x_1, \ldots, x_n]$. Assume that the following conditions are satisfied:

1. *$f_{0r}(x_1, \ldots, x_n)$ is homogeneous of degree, say, $d_r \geq 1$.*
2. *Every monomial $x_1^{i_1} \cdots x_n^{i_n}$ in $F_r(x_1, \ldots, x_n)$ is of degree at least d_r (this, in particular, implies $F_r(0, \ldots, 0) = 0$).*
3. *For every $r = 1, \ldots, n$ there exist $h_{1r}, \ldots, h_{nr} \in \mathbb{Z}_p[x_1, \ldots, x_n]$ such that $h_{1r} \cdot f_{01} + \cdots + h_{nr} \cdot f_{0n} = H_r \in \mathbb{Z}_p[x_r]$ and the only solution to the congruence $H_r(x) \equiv 0 \pmod{p}$ is $x \equiv 0 \pmod{p}$ (this, in particular, implies that H_r is a non-zero polynomial $\bmod p$).*

Then, the only solution in p-adic integers of the system $F_r(x_1, \ldots, x_n) = 0$, $(r = 1, \ldots, n)$ is the zero solution.

Proof. Suppose $F_r(x_1, ..., x_n) = 0$ for $r = 1, ..., n$, where $x_i \in \mathbf{Z}_p$ are not all zero. Then

$$f_{0r}(x_1, ..., x_n) \equiv 0 \pmod{p}, \quad r = 1, ..., n$$

so that by hypothesis (3),

$$H_r(x_r) \equiv 0 \pmod{p}, \quad r = 1, ..., n,$$

that is, also by hypothesis (3),

$$x_r \equiv 0 \pmod{p}, \quad r = 1, ..., n.$$

Thus $p^{\alpha_r} || x_r$, $\alpha_r \geq 1$ (with convention that $\alpha_r = \infty$ if $x_r = 0$). Define the integer j in the range $1 \leq j \leq n$ by $\alpha_j = \min(\alpha_1, \alpha_2, ..., \alpha_n) = \alpha$. (The integer j exists since at least one α_r is finite). Now put $x_r = p^\alpha X_r$, $r = 1, ..., n$, where $X_r \in \mathbf{Z}_p$, and $p \not| X_j$.

Then

$$F_r(x_1, ..., x_n) = 0, \quad r = 1, ..., n,$$

implies

$$\sum_{i=0}^{\infty} p^i f_{ir}(p^\alpha X_1, ..., p^\alpha X_n) = 0, \quad r = 1, ..., n,$$

that is,

$$p^{\alpha d_r}[f_{0r}(X_1, ...X_n) + \sum_{i=1}^{\infty} p^i g_{ir}(X_1, ..., X_n)] = 0, \quad r = 1, ..., n,$$

where $g_{ir}(X_1, ..., X_n) \in \mathbf{Z}_p[X_1, ..., X_n]$, using hypotheses (1) and (2). Thus

$$f_{0r}(X_1, ...X_n) + \sum_{i=1}^{\infty} p^i g_{ir}(X_1, .., X_n)) = 0, \quad r = 1, ..., n,$$

so that

$$f_{0r}(X_1, ..., X_n) \equiv 0 \pmod{p}, \quad r = 1, ..., n,$$

whence by hypothesis (3),

$$H_r(X_r) \equiv 0 \pmod{p}, \quad r = 1, ..., n.$$

In particular,

$$H_j(X_j) \equiv 0 \pmod{p},$$

so that $X_j \equiv 0 \pmod{p}$, by hypothesis (3), contrary to assumption. □

Remarks (1) If for every $r = 1, \ldots, n$, $d_r = 1$, hence $f_{0r} = a_{1r}x_1 + \cdots + a_{nr}$ (say), then the conditions of the theorem are equivalent to the non-vanishing mod$p$ of the determinant of the matrix (a_{ir}).
(2) When $n = 2$, at least the existence of the polynomials h_{1r}, h_{2r}, $(r = 1, 2)$ is guaranteed by the basic theory of resultants; in that case, $H_1(x_1)$ is the resultant of the polynomials $f_{01}(x_1, x_2), f_{02}(x_1, x_2)$ with respect to the variable x_2, and analogously for $H_2(x_2)$.

Application of Theorem 3 to (29)

A Mordell-Weil basis for the elliptic curve (29) over $\mathbb{Q}(\phi)$ is formed by the generators of infinite order $P_1 = (1, \frac{1}{2}\phi^2), P_2 = (\frac{1}{2}\phi + \frac{1}{2}\phi^2 - \frac{1}{4}\phi^3, 1 - \frac{3}{2}\phi^2)$ (see section 4.10 in the appendix to [2]) and the generator $T = (0, 0)$ of the torsion subgroup. We define $Q_1 = P_1 + 8P_2$, $Q_2 = 24P_2$. Note that $\{Q_1, P_2\}$ remains a basis for the torsion-free part of the group of rational points of (29) over $\mathbb{Q}(\phi)$, therefore any non-zero point $(X, Y) \in \mathcal{E}_{10}(\mathbb{Q}(\phi))$ can be written as

$$kP_2 + \epsilon T + n_1 Q_1 + n_2 Q_2\,, \quad n_1, n_2 \in \mathbb{Z}\,,\ k \in \{-11, \ldots, 12\}\,,\ \epsilon \in \{0, 1\}\,, \qquad (38)$$

and n_1, n_2, k, ϵ not all zero.

Note that Assumption 1 at the beginning of section 4.4 is fulfilled with $p = 3$ and $\beta = 6\phi + \phi^3, \gamma = -4\phi - \phi^3$. Assumption 2 is then fulfilled for the points Q_1, Q_2 defined above. In (38) we put $P = kP_2 + \epsilon T$. There are $24 \cdot 2 = 48$ possibilities for P, with points other than for $k = \epsilon = 0$ being "finite points". The generic point $(X, Y) \in \mathcal{E}_{10}(\mathbb{Q}(\phi))$ has the form $P + n_1 Q_1 + n_2 Q_2$, and hence Assumption 3 is also fulfilled. We are interested in finding all points (X, Y) as above, that satisfy condition (32). Therefore, if at least one of k, ϵ is non-zero, we may assume, since $T = -T$, that $k \in \{1, \ldots, 12\}$ if $\epsilon = 0$ and $k \in \{0, \ldots, 12\}$ if $\epsilon = 1$, reducing thus to $1 + 12 + 13 = 26$ the possibilities for the point P.

Following the method of Flynn and Wetherell [13] as described in section 4 of [1], we have (in the notation of [1])

$$\begin{aligned} z(Q_1) &= 33 + 240\phi + 33\phi^2 + 93\phi^3 + O(3^5) \in \mathcal{M} \\ z(Q_2) &= 213 + 234\phi + 105\phi^2 + 144\phi^3 + O(3^5) \in \mathcal{M}\,. \end{aligned}$$

The "addition law" in the *formal group* of our elliptic curve is given by

$$\begin{aligned} \mathcal{F}(z_1, z_2) =& z_1 + z_2 + (\frac{1}{2}\phi^2 + 1)z_1 z_2^2 + (\frac{1}{2}\phi^2 + 1)z_1^2 z_2 + (\phi^2 - 2)z_1 z_2^4 \\ &+ (2\phi^2 - 2)z_1^2 z_2^3 + (2\phi^2 - 2)z_1^3 z_2^2 + (\phi^2 - 2)z_1^4 z_2 + \cdots \end{aligned}$$

The logarithmic and exponential series in the formal group are

$$\begin{aligned} \log t =& t + (-\frac{1}{6}\phi^2 - \frac{1}{3})t^3 + \frac{2}{5}t^5 + O(t^7) \\ \exp t =& t + (\frac{1}{6}\phi^2 + \frac{1}{3})t^3 + \frac{4}{15}t^5 + O(t^7) \end{aligned}$$

For any point Q on the elliptic curve we will use the notation $X(Q)$ for the X-coordinate of the point Q. For any finite points $P = (X_0, Y_0)$ and R of our elliptic curve we express $\beta X(P + R) + \gamma$ (with $\beta = 6\phi + \phi^3$ and $\gamma = -4\phi - \phi^3$) as a

formal power series of $z(R)$ with coefficients in $\mathbb{Z}[\phi, X_0, Y_0]$:

$$\begin{aligned}\beta X(P+R)+\gamma = &(X_0-1)\phi^3+(6X_0-4)\phi+(2Y_0\phi^3+12Y_0\phi)\,z(R)\\ &+[(3X_0^2-4X_0)\phi^3+(4-16X_0+18X_0^2)\phi]\,z(R)^2\\ &+[(4Y_0X_0-4Y_0)\phi^3+(24Y_0X_0-16Y_0)\phi]\,z(R)^3\\ &+[(4X_0-2+Y_0^2+4X_0^3-12X_0^2)\phi^3\\ &\quad+(24X_0^3-48X_0^2+32X_0-4+6Y_0^2)\phi]\,z(R)^4+O(z(R)^5)\end{aligned} \tag{39}$$

We also express the inverse of $\beta X(R)+\gamma$ as a formal power series in $z(R)$:

$$\frac{1}{\beta X(R)+\gamma}=\frac{\phi^3+2\phi}{16}z(R)^2-\frac{\phi}{8}z(R)^4+\frac{5\phi^3+2\phi}{32}z(R)^6+O(z(R)^8) \tag{40}$$

We have the 3-adic expansions

$$\begin{aligned}\log z(Q_1)&=3(32+35\phi+50\phi^2+61\phi^3)+O(3^5)\in 3\mathbb{Z}_3[\phi]\\ \log z(Q_2)&=3(47+38\phi^2)+3^2(8\phi+7\phi^3)+O(3^5)\in 3\mathbb{Z}_3[\phi]\ .\end{aligned}$$

Let n_1, n_2 be integers and set $R=n_1Q_1+n_2Q_2$. From section 4 of [1] we know that

$$z(R)=z(n_1Q_1+n_2Q_2)=\exp(n_1\log z(Q_1)+n_2\log z(Q_2))\in 3\mathbb{Z}_3\langle n_1,n_2\rangle[\phi]\ .$$

This can be easily computed $\bmod 3^5$; we need consider only the first three terms of the exponential series, in view of the fact that $\log z(Q_1), \log z(Q_2)\in 3\mathbb{Z}_3[\phi]$.

$$\begin{aligned}z(R)\bmod 3^5=&216n_1n_2^2+81n_1^2n_2+96n_1+141n_2+180n_1^3+153n_2^3+81n_2^4n_1\\ &+162n_2^5+81n_2n_1^4+162n_2^2n_1^3\\ &+(135n_1^3+162n_2^3+72n_2+105n_1+81n_2^4n_1+216n_1n_2^2\\ &+81n_2n_1^4+81n_2^3n_1^2+108n_1^2n_2)\phi\\ &+(150n_1+114n_2+72n_2^3+162n_2^5+81n_2^4n_1+135n_1n_2^2\\ &+126n_1^3+108n_1^2n_2+81n_2^3n_1^2+162n_2^2n_1^3)\phi^2\\ &+(81n_2^3+81n_1^5+183n_1+63n_2+72n_1^3+162n_2^3n_1^2\\ &+162n_2^4n_1+162n_2^2n_1^3+135n_1^2n_2+189n_1n_2^2)\phi^3\end{aligned} \tag{41}$$

As noted in (2), substitution of the above value for $z(R)$ in (39) and (40) gives, after reduction $\bmod 3^5$, an element in $\mathbb{Z}\langle n_1,n_2\rangle[\phi,X_0,Y_0]$ and $\mathbb{Z}\langle n_1,n_2\rangle[\phi]$, respectively (the formulas are too long, especially the first one, to be included here). This is of the form

$$\theta_0(n_1,n_2)+\theta_1(n_1,n_2)\phi+\theta_2(n_1,n_2)\phi^2+\theta_3(n_1,n_2)\phi^3\ , \tag{42}$$

where $\theta_i(x,y)\in\mathbb{Z}[x,y]$ and, in the first case, with coefficients depending on X_0, Y_0.

Notation. In the sequel we assume that (X, Y) is a point on the curve $\mathcal{E}_{10}$, such that X satisfies condition (32). We put $R = n_1Q_1 + n_2Q_2$, with $n_1, n_2 \in \mathbb{Z}$. Note that, the typical form of (X, Y) is either $(X, Y) = P + R$ with $P = (X_0, Y_0)$ belonging to the set of 25 "finite" points mentioned at the beginning of this section, or $(X, Y) = R$.

Case 1: $(X, Y) = P + R$. We recall that $P = (X_0, Y_0) = kP_2 + \epsilon T$, $k = 0, 1, \ldots, 12$, $\epsilon = 0, 1$. Suppose first $\epsilon = 1$. Using the computer we find, for every specific P, an explicit expression for the form (42) for $\beta X + \gamma \pmod{3^5}$. In every case but $k = 4$, we find out that $\theta_i(n_1, n_2) \not\equiv 0 \pmod 3$ for at least one i, hence $\beta X + \gamma$ cannot be a rational number. When $k = 4$, we compute $\theta_1(n_1, n_2) \equiv 6+6n_1+6n_2 \pmod{3^2}$ and $\theta_3(n_1, n_2) \equiv 3n_1+3n_2 \pmod{3^2}$, therefore the simultaneous vanishing of $\theta_1(n_1, n_2)$ and $\theta_3(n_1, n_2)$ is impossible. This leads to the conclusion that $\beta X + \gamma$ cannot be a rational number. Next, consider the case $\epsilon = 0$. In every case but $k = 2, 10$, we see that $\theta_i(n_1, n_2) \not\equiv 0 \pmod 3$ for at least one i, hence $\beta X + \gamma$ cannot be a rational number.

The cases $k = 2, 10$ need a deeper treatment. Working p-adically with $p = 3$ we apply Theorem 3 in order to solve in 3-adic integers the system

$$\theta_3(n_1, n_2) = 0,\ \theta_2(n_1, n_2) = 0 \quad n_1, n_2 \in \mathbb{Z}_3\ . \tag{43}$$

Case 1.1: $P = 2P_2$. We are looking for points $(X, Y) = 2P_2 + n_1Q_1 + n_2Q_2$ such that X satisfies condition (32). Note that, for $(n_1, n_2) = (0, 0)$ this is satisfied. Indeed, then

$$(X, Y) = 2P_2 = (\frac{1}{2} - \frac{1}{2}\phi + \frac{1}{4}\phi^2 - \frac{1}{4}\phi^3, \frac{1}{2} - \frac{1}{4}\phi - \frac{1}{8}\phi^3)$$

and we check that $\beta X + \gamma = -4$, as required. This means that $(n_1, n_2) = (0, 0)$ is a solution to the system (43). Keeping in mind this solution we define

$$F_1(n_1, n_2) = \frac{1}{3}\theta_3(n_1, n_2)\ ,\ F_2(n_1, n_2) = \frac{1}{3}\theta_2(n_1, n_2)$$

and, using theorem 3, we will show that $(n_1, n_2) = (0, 0)$ is the only solution of the system $F_1 = 0, F_2 = 0$ in 3-adic integers. We compute

$$\begin{aligned} F_1(n_1, n_2) =& 2n_1 + 3(n_1^3 + n_1^2 + n_1 + n_2 + 2n_2^2) \\ &+ 3^2(n_2 + 2n_1 + n_2^3 + 2n_2^2 + n_2^4 + 2n_1n_2 + 2n_1n_2^2) + 3^3(\cdot)\ , \end{aligned}$$

where $(\cdot)$ denotes a series in $\mathbb{Z}\langle n_1, n_2\rangle$ with zero constant term. Also,

$$\begin{aligned} F_2(n_1, n_2) =& n_1 + n_2 + 3(2n_1^3 + n_1^2 + 2n_1n_2 + n_1 + n_2^3) \\ &+ 3^2(2n_1^2 + 2n_2^3 + 2n_2^2 + 2n_1^2n_2 + 2n_1n_2 + n_1n_2^2 + 2n_1n_2^3) + 3^3(\cdot)\ , \end{aligned}$$

where $(\cdot)$ is as above. Actually the essential terms are $f_{01} = 2n_1$ and $f_{02} = n_1+n_2$, with corresponding determinant of their coefficients

$$\begin{vmatrix} 2 & 0 \\ 1 & 1 \end{vmatrix} .$$

This is non-zero mod 3, hence, by remark (1) following theorem 3, the only solution to our system is $(n_1, n_2) = (0, 0)$. This corresponds to the point $2P_2$ on the curve $\mathcal{E}_{10}$ with X-coordinate $\frac{1}{2} - \frac{1}{2}\phi + \frac{1}{4}\phi^2 - \frac{1}{4}\phi^3$. Then, in section 4.1.2 $(a, b) = (1, -4)$ which does not furnish us with a solution of equation (5).

Case 1.2: $P = 10P_2$. Now we are looking for points $(X, Y) = 10P_2 + n_1Q_1 + n_2Q_2$ such that X satisfies condition (32). Note that, for $(n_1, n_2) = (2, -1)$ the condition is satisfied. Indeed, then

$$(X, Y) = 10P_2 + 2Q_1 - Q_2 = 2P_1 + 2P_2 = (\frac{1}{2} + \frac{1}{2}\phi + \frac{1}{4}\phi^2 + \frac{1}{4}\phi^3, -\frac{1}{2} - \frac{1}{4}\phi - \frac{1}{8}\phi^3)$$

and we check that $\beta X + \gamma = 4$, as required. In particular, we conclude that $(n_1, n_2) = (2, -1)$ is a solution to (43). Therefore, we put $n_1 = x_1+2, n_2 = x_2-1$, we define

$$\begin{aligned} F_1(x_1, x_2) =& \frac{1}{3}\theta_3(n_1, n_2) = \frac{1}{3}\theta_3(x_1 + 2, x_2 - 1) , \\ F_2(x_1, x_2) =& \frac{1}{3}\theta_2(n_1, n_2) = \frac{1}{3}\theta_2(x_1 + 2, x_2 - 1) \end{aligned}$$

and we will show, using theorem 3, that $(x_1, x_2) = (0, 0)$ is the only solution in 3-adic integers to the system $F_1 = 0, F_2 = 0$. We compute

$$\begin{aligned} F_1(x_1, x_2) =& 2x_1 + 3(2x_2x_1 + 2x_2^2 + x_1^3) + 3^2(\cdot) \\ F_2(x_1, x_2) =& x_1 + x_2 + 3(2x_2x_1 + x_2^3) + 3^2(\cdot) , \end{aligned}$$

where $(\cdot)$ denotes a series in $\mathbb{Z}\langle n_1, n_2\rangle$ with zero constant term. As in case 1.1, the determinant of the coefficients of the first-degree terms $2x_1$ and $x_1 + x_2$ is non-zero mod3, therefore $(x_1, x_2) = (0, 0)$ is the only solution of the system in 3-adic integers. It follows that, in case 1.2, $(n_1, n_2) = (2, -1)$ is the only possible solution of the system (43). This gives a point on the curve $\mathcal{E}_{10}$ with X-coordinate $\frac{1}{2} + \frac{1}{2}\phi + \frac{1}{4}\phi^2 + \frac{1}{4}\phi^3$. This, in turn, implies $(a, b) = (4, 1)$ in section 4.1.2, which does not provide with a solution of equation (5).

Case 2: $(X, Y) = R$. We recall that $R = n_1Q_1 + n_2Q_2$, with $n_1, n_2 \in \mathbb{Z}$. In this case we are looking for points $(X, Y) = n_1Q_1 + n_2Q_2$ with X such that condition (32) be satisfied. More generally, we demand that the right-hand side of (40) be rational. For $(n_1, n_2) = (0, 0)$ this condition is satisfied. Indeed, then $R = \mathcal{O}$, $z(R) = 0$ (by the definition of the function z; see section 4 of [1]), and the right-hand side of (40) is zero.

As mentioned immediately after (41), substitution of $z(R)$ in (40) from its value in (41) gives

$$\frac{1}{\beta X+\gamma}=\theta_0(n_1,n_2)+\theta_1(n_1,n_2)\phi+\theta_2(n_1,n_2)\phi^2+\theta_3(n_1,n_2)\phi^3\ ,$$

hence, in order that the left-hand side be a rational number it is necessary that $\theta_1(n_1,n_2)=\theta_2(n_1,n_2)=\theta_3(n_1,n_2)=0$. We will consider the system

$$\theta_3(n_1,n_2)=0,\ \theta_1(n_1,n_2)=0\ \ n_1,n_2\in\mathbb{Z}_3\ , \tag{44}$$

which, according to our discussion a few lines above, has the solution $(n_1,n_2)=(0,0)$, and will show, using theorem 3 that this is its only solution in 3-adic integers. We set

$$F_1(n_1,n_2)=\frac{1}{9}\theta_3(n_1,n_2)\ ,\ F_2(n_1,n_2)=\frac{1}{9}\theta_1(n_1,n_2)$$

and we compute:

$$\begin{aligned}F_1(n_1,n_2)=&2n_1^2+3(n_1^4+2n_1^2+n_1n_2)+3^2(\cdot)\\ F_2(n_1,n_2)=&n_1^2+n_1n_2+2n_2^2+3(n_1^3n_2+n_1n_2^3+n_2^2+n_2^4)+3^2(\cdot)\ ,\end{aligned}$$

where $(\cdot)$ denotes an element of $\mathbb{Z}\langle n_1,n_2\rangle$ all of whose terms are of degree at least 2. Now, in the notation of theorem 3, $f_{01}=2n_1^2, f_{02}=n_1^2+n_1n_2+2n_2^2$. We can obviously take $h_{11}=1, h_{21}=0, H_1=2n_1^2$. As for H_2, we can take it as the resultant of f_{01}, f_{02} with respect to n_1, finding thus $H_2=16n_2^4$ (here, $h_{12}=2n_2n_1-2n_2^2, h_{22}=-4n_2n_1+8n_2^2$, but we do not actually need these polynomials). In view of the shape of the polynomials H_1, H_2, it follows by theorem 3 that $(n_1,n_2)=(0,0)$ is the only solution of $F_1(n_1,n_2)=0, F_2(n_1,n_2)=0$ in 3-adic integers and this solution corresponds to the zero point on the curve $\mathcal{E}_{10}$ which is of no interest for our initial problem.

Summing up the previous results, we have proved the following

Proposition 4. *In the notation of section 4.2.4, the only points (X,Y) on $\mathcal{E}_{10}(\mathbb{Q}(\phi))$ satisfying the condition $\beta X+\gamma\in\mathbb{Q}$ ($\beta=6\phi+\phi^3, \gamma=-4\phi-\phi^3$) are $\pm 2P_2, \pm(2P_1+2P_2)$. No one of them furnishes a solution to equation (5), hence no solution to our initial problem can be obtained from the elliptic curve $\mathcal{E}_{10}$.*

References

[1] A. Bremner and N. Tzanakis, Lucas sequences whose 12th or 9th term is a square, *J. Number Th.* (to appear).

[2] A. Bremner and N. Tzanakis, Lucas sequences whose 8th term is a square, extended version with appendix, http://www.math.uoc.gr/~tzanakis/Papers/appendix.pdf

[3] N. Bruin, `http://www.cecm.sfu.ca/~bruin/ell.shar`

[4] N. Bruin, `http://www.cecm.sfu.ca/~bruin/malgae.tgz`

[5] N. Bruin, The primitive solutions to $x^3 + y^9 = z^2$, 2003, `http://arxiv.org/abs/math.NT/0311002`, with related transcript `http://www.cecm.sfu.ca/ nbruin/eq239`

[6] N. Bruin and N.D. Elkies, Trinomials ax^7+bx+c and ax^8+bx+c with Galois Groups of Order 168 and $8*168$, *Algorithmic Number Theory, 5th International Symposium, ANTS-V, (Claus Fieker, David R. Kohel Eds.), Lecture Notes in Computer Science* **2369** Springer (2002), 172-188.

[7] N. Bruin, Chabauty methods and covering techniques applied to generalized Fermat equations, *CWI Tract*, vol. 133, Stichtung Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam (2002), Dissertation, University of Leiden, Leiden (1999).

[8] N. Bruin, Chabauty methods using elliptic curves, *J. reine angew. Math.*, **562** (2003), 27-49.

[9] J.W.S. Cassels, *Local Fields*, LMS Student Texts **3**, Cambridge University Press, Cambridge and London 1986.

[10] C. Chabauty, Sur les points rationnels des courbes algébriques de genre supérieur à l'unité, *C. R. Acad. Sci. Paris*, **212**, 1941, 882-885.

[11] J.H.E. Cohn, On square Fibonacci numbers, *J. London Math. Soc.* **39** (1964), 537-541.

[12] S. Duquesne, Rational points on hyperelliptic curves and an explicit Weierstrass preparation theorem, *Manuscripta Math.* **108** (2002), 191-204.

[13] E.V. Flynn and J.L. Wetherell, Finding rational points on bielliptic genus 2 curves, *Manuscripta Math.* **100** (1999), 519-533.

[14] M. Kida, *TECC manual version 2.4*, The University of Electro-Communications, September 2000.

[15] P. Ribenboim and W.L. McDaniel, *The square terms in Lucas sequences*, J. Number Theory, **58**, 1996, 104-123.

[16] P. Ribenboim and W.L. McDaniel, *Squares in Lucas sequnces having an even first parameter*, Colloq. Math., **78**, 1998, 29-34.

[17] N. Robbins, On Pell numbers of the form PX^2, where P is prime, *Fibonacci Quart.*, **4** (1984), 340-348.

[18] S. Siksek, Infinite descent on elliptic curves, *Rocky Mountain J. Math.*, **. 25** (1995), 1501-1538.

[19] J.H. Silverman, Computing heights on elliptic curves, *Math. Comp.* **51** (1988), 339-358.

[20] J.H. Silverman, The difference between the Weil height and the canonical height on elliptic curves, *Math. Comp.* **55** (1990), 723-743.

[21] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, Berlin and New York, 1986.

[22] D. Simon, *http://www.math.unicaen.fr/ simon/ell.gp*

[23] Th. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, 8de Skand. mat. Kongr., Stockholm, 1934.

[24] T.N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Univ. Press, Cambridge, 1986.

[25] T. Sugatani, Rings of convergent power series and Weierstrass preparation theorem, *Nagoya Math. J.*, **81** (1981), 73-78.

5 Appendix: The Mordell-Weil bases

Notation: let ν be a non-Archimedean absolute value on K, where K denotes K_1 or K_2, as appropriate, and let

$$\mathrm{ord}_\nu : K_\nu^* \to \mathbf{Z}$$

be the corresponding normalized valuation: so that if the residue field at ν has order q_ν, then

$$\log |x|_\nu = -\frac{1}{[K_\nu : \mathbf{Q}_\nu]} \mathrm{ord}_\nu(x) \log(q_\nu)$$

for all $x \in K_\nu^*$. Equivalently,

$$|x|_\nu^{[K_\nu:\mathbf{Q}_\nu]} = q_\nu^{-\mathrm{ord}_\nu(x)},$$

guaranteeing the product identity (over all non-Archimedean and Archimedean absolute values)

$$\prod_\nu |x|_\nu^{[K_\nu:\mathbf{Q}_\nu]} = 1.$$

The Archimedean valuation of $\mathbb{Q}$ has three extensions to K, with $K_{\infty_1} = K_{\infty_2} = \mathbf{R}$ and $K_{\infty_3} = \mathbf{C}$. We have $|x|_{\infty_1} = |x(\theta)|$ (resp, $|x(\phi)|$), $|x|_{\infty_2} = |x(-\theta)|$, (resp. $|x(-\phi)|$), and $|x|_{\infty_3} = |x(i/\theta)|$ (resp. $|x(2i/\phi)|$) - equivalently, $|x|_{\infty_3}^2 = |x(i/\theta)x(-i/\theta)|$ (resp. $|x(2i/\phi)x(-2i/\phi)|$).
Define the indices $n_\nu = |K_\nu : \mathbb{Q}_\nu|$. Then

$$\boxed{n_{(1+\theta)} = 4, \qquad n_\pi = 4, \qquad n_{\infty_1} = n_{\infty_2} = 1, \quad n_{\infty_3} = 2.}$$

The discriminants and Kodaira reduction types above 2 are given in the following table; we also include the coefficients $\mu_{(1+\theta)}$ and μ_π, in Siksek's notation:

Curve	Discriminant	Kodaira reduction type above 2	$\mu_{(1+\theta)}$	μ_π	
(8):	$-\epsilon_1^{-14}\epsilon_2^6(1+\theta)^{18}$	II	0		
(10):	$-\epsilon_1^{-14}\epsilon_2^{12}(1+\theta)^{18}$	II	0		
(13):	$-\epsilon_1^{-4}\epsilon_2^6(1+\theta)^{18}$	II	0		
(15):	$-\epsilon_1^{-4}\epsilon_2^{12}(1+\theta)^{18}$	II	0		
(18):	$-\epsilon_1^{-2}\epsilon_2^{-12}\pi^{24}$	I_4^*		1/4	
(20):	$-\epsilon_1^{4}\epsilon_2^{-12}\pi^{24}$	I_6^*		1/4	
(22):	$-\epsilon_1^{-2}\epsilon_2^{-6}\pi^{24}$	I_4^*		1/4	
(24):	$-\epsilon_1^{4}\epsilon_2^{-6}\pi^{24}$	I_6^*		1/4	
(27):	$-\epsilon_1^{2}\epsilon_2^{-12}\pi^{24}$	I_4^*		1/4	
(29):	$-\epsilon_1^{8}\epsilon_2^{-12}\pi^{24}$	I_6^*		1/4	
(33):	$-\epsilon_1^{2}\epsilon_2^{-6}\pi^{24}$	I_4^*		1/4	
(35):	$-\epsilon_1^{8}\epsilon_2^{-6}\pi^{24}$	I_6^*		1/4	

We now make some remarks about the minimal polynomial of $x(Q)$ for $Q \in E(K)$, with height $H(Q)$ bounded above by B, say. Put $x_1 = x(Q)$. If $|\mathbb{Q}(x_1) : \mathbb{Q}| = 4$, let x_i, $i = 1, ..., 4$ denote the four conjugates of x_1, with minimum polynomial of x_1 being

$$x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = (x - x_1)(x - x_2)(x - x_3)(x - x_4).$$

Since

$$|x_1| = |x_1|_{\infty_1} \leq \max\{1, |x_1|_{\infty_1}\} \leq H(x_1) < B,$$

then

$$|a_1| = |x_1 + x_2 + x_3 + x_4| \leq |x_1| + |x_2| + |x_3| + |x_4| < 4B,$$

using the fact that conjugate points have equal height. In this way, we have

$$|a_1| < 4B, \quad |a_2| < 6B^2, \quad |a_3| < 4B^3, \quad |a_4| < B^4. \tag{45}$$

Similarly, if $|\mathbb{Q}(x_1) : \mathbb{Q}| = 2$, then the minimal polynomial of x_1 is of type $x^2 + a_1 x + a_2$, where

$$|a_1| < 2B, \qquad |a_2| < B^2. \tag{46}$$

Finally, if $|\mathbb{Q}(x_1) : \mathbb{Q}| = 1$, then the minimal polynomial of x_1 is of type $x + a_1$, where

$$|a_1| < B. \tag{47}$$

5.1 The curve $\mathcal{E}_1$ at (8)

¿From the table of Kodaira reduction types, we have that (in Siksek's notation) $\mu_\nu = 0$ except for

$$\boxed{\mu_{\infty_1} = \mu_{\infty_2} = \mu_{\infty_3} = \tfrac{1}{3}.}$$

Further,

$$\epsilon_\nu^{-1} = \inf_{(X,Y)\in E(K_\nu)} \frac{\max(|f(X)|_\nu, |g(X)|_\nu)}{\max(1, |X|_\nu)^4}$$

with

$$f(X) = 4X^3 - 4(\theta + \theta^2)X^2 + 4(1 + \theta + \theta^3)X, \qquad g(X) = (X^2 - (1 + \theta + \theta^3))^2.$$

Siksek gives a method for computing the ϵ_ν. At ∞_1,

$$\epsilon_{\infty_1}^{-1} = \inf_{(X,Y)\in E(\mathbf{R})} \frac{\max(|f(X)|, |g(X)|)}{\max(1, |X|)^4},$$

and the infimum needs to be taken over $X \in \mathbf{R}$ such that $f(X) \geq 0$, that is, over $[0, \infty)$. This infimum occurs at the root 4.275236449758861... of $f(X) - g(X) = 0$, and has value 0.80190401917789682199..., so that

$$\boxed{\epsilon_{\infty_1} = 1.24703203386508649515...}.$$

At ∞_2,

$$\epsilon_{\infty_2}^{-1} = \inf_{(X,Y)\in E(\mathbf{R})} \frac{\max(|\bar{f}(X)|, |\bar{g}(X)|)}{\max(1, |X|)^4},$$

where

$$\bar{f}(X) = 4X^3 - 4(-\theta + \theta^2)X^2 + 4(1 - \theta - \theta^3)X, \quad \bar{g}(X) = (X^2 - (1 - \theta - \theta^3))^2,$$

with infimum taken over $X \in \mathbf{R}$ such that $f(X) \geq 0$, that is, over $[0, \infty)$. This infimum occurs at the root 0.021005066751861... of $\bar{f}(X) - \bar{g}(X) = 0$, and has value 0.00798861744730799360... so that

$$\boxed{\epsilon_{\infty_2} = 125.17810579814161228611...}.$$

At ∞_3,

$$\epsilon_{\infty_3}^{-1} = \inf_{(X,Y) \in E(\mathbf{C})} \frac{\max(|F(X)|, |G(X)|)}{\max(1, |X|)^4},$$

where

$$F(X)^2 = 16X^2(X^4 + (4 + 2\theta^2)X^3 + (9 + 3\theta^2)X^2 + (10 + 4\theta^2)X + (5 + 2\theta^2)),$$

$$G(X) = (X^4 - 2X^2 + (5 + 2\theta^2)).$$

The infimum occurs at the root $-1.45508613805... - 0.5449200796689308...i$ of $|F(z)| = |G(z)|$, with value 0.67959006502634452483776 98... (on the unit circle, the minimum taken exceeds 4). Thus

$$\boxed{\epsilon_{\infty_3} = 1.47147530763451446602571 7...}$$

Putting the above together results in

$$\begin{aligned} h(P) - 2\hat{h}(P) \quad \leq \quad & \frac{1}{4}(\frac{1}{3} \cdot 1 \cdot \log(1.24703203386508649515) \\ & + \frac{1}{3} \cdot 1 \cdot \log(125.17810579814161228611) \\ & + \frac{1}{3} \cdot 2 \cdot \log(1.4714753076345144660257)), \end{aligned}$$

that is,

$$h(P) - 2\hat{h}(P) \leq 0.485252911746822...$$

Suppose now the point G_1 at (9) is not a generator. We easily check that G_1 is not divisible by 2 in $E(K)$, and so $G_1 = mQ$ for $m \geq 3$ and $Q \in E(K)$. Note that since $(1 + \theta)^2 x(G_1) \in \mathcal{O}_K$, it follows that $(1 + \theta)^2 x(Q) \in \mathcal{O}_K$. Then

$$h(Q) \leq 0.485252911746822 + 2\hat{h}(Q) < 0.485252911746822 + 2\hat{h}(G_1)/m^2 < 0.614184$$

so that

$$H(Q) < 1.84815.$$

Suppose first that $x(Q) \in \mathcal{O}_\mathcal{K}$. Write $H(Q) < B$. If $|\mathbb{Q}(x(Q)) : \mathbb{Q}| = 4$, then by direct computation, the minimum polynomial of $x(Q)$ is of type $X^4 + 4c_1X^3 + 2c_2X^2 + 4c_3X + c_4$, where $c_i \in \mathbb{Z}$, $i = 1, .., 4$. Similarly, if $|\mathbb{Q}(x(Q)) : \mathbb{Q}| = 2$, then the minimal polynomial of $x(Q)$ is of type $X^2 + 2c_1X + c_2$, with $c_i \in \mathbb{Z}$. From (45), (46), (47), we therefore have to investigate the following polynomials:

- $X^4 + 4c_1X^3 + 2c_2X^2 + 4c_3X + c_4$, $c_i \in \mathbb{Z}$, $|c_1| < B$, $|c_2| < 3B^2$, $|c_3| < B^3$, $|c_4| < B^4$.
- $X^2 + 2c_1X + c_2$, $c_i \in \mathbb{Z}$, $|c_1| < B$, $|c_2| < B^2$.
- $X + c_1$, $c_1 \in \mathbb{Z}$, $|c_1| < B$.

Suppose second that $x(Q) = u/(1+\theta)^2$, where $u \in \mathcal{O}_K$, and $u \equiv 1 \pmod{(1+\theta)}$. If $|\mathbb{Q}(x(Q)) : \mathbb{Q}| = 4$, then by direct computation, the minimum polynomial of $x(Q)$ is of type $X^4+4c_1X^3+c_2X^2+2c_3X+\frac{c_4}{4}$, where $c_i \in \mathbb{Z}$, and $c_2 \equiv c_4 \equiv 1 \pmod 2$. Similarly, if $|\mathbb{Q}(x(Q)) : \mathbb{Q}| = 2$, then the minimal polynomial of $x(Q)$ is of type $X^2 + 2c_1X + \frac{c_2}{4}$, where $c_i \in \mathbb{Z}$, and $c_2 \equiv 3 \pmod 4$. As above, we then have to investigate polynomials:
• $X^4 + 4c_1X^3 + c_2X^2 + 2c_3X + \frac{c_4}{4}$, $c_i \in \mathbb{Z}$, $c_2 \equiv c_4 \equiv 1 \pmod 2$,

$$|c_1| < B, |c_2| < 6B^2, |c_3| < 2B^3, |c_4| < 4B^4.$$

• $X^2 + 2c_1X + \frac{c_2}{4}$, $c_i \in \mathbb{Z}$, $c_2 \equiv 3 \pmod 4$, $|c_1| < B$, $|c_2| < 4B^2$.

Numerically, we have to investigate polynomials:
• $X^4 + 4c_1X^3 + 2c_2X^2 + 4c_3X + c_4$, $c_i \in \mathbb{Z}$, $|c_1| \le 1$, $|c_2| \le 10$, $|c_3| \le 6$, $|c_4| \le 11$
• $X^2 + 2c_1X + c_2$, $c_i \in \mathbb{Z}$, $|c_1| \le 1$, $|c_2| \le 3$
• $X + c_1$, $c_1 \in \mathbb{Z}$, $|c_1| \le 1$
and
• $X^4 + 4c_1X^3 + c_2X^2 + 2c_3X + \frac{c_4}{4}$, $c_i \in \mathbb{Z}$, $c_2 \equiv c_4 \equiv 1 \pmod 2$, $|c_1| \le 1$, $|c_2| \le 20$, $|c_3| \le 12$, $|c_4| \le 46$
• $X^2 + 2c_1X + \frac{c_2}{4}$, $c_i \in \mathbb{Z}$, $c_2 \equiv 3 \pmod 4$, $|c_1| \le 1$, $|c_2| < 13$.
Each polynomial has to be tested to see if a root can be the X-coordinate of a point in $\mathcal{E}_1(K)$. Computation shows that in the given range, only the points $\pm G_1$ arise. It follows that G_1 is indeed a generator of the group of points defined over K.

5.2 The curve $\mathcal{E}_2$ at (10)

¿From the table of Kodaira reduction types, we have $\mu_\nu = 0$ except for

$$\boxed{\mu_{\infty_1} = \mu_{\infty_2} = \mu_{\infty_3} = \tfrac{1}{3}.}$$

Further,

$$\epsilon_\nu^{-1} = \inf_{(X,Y)\in E(K_\nu)} \frac{\max(|f(X)|_\nu, |g(X)|_\nu)}{\max(1, |X|_\nu)^4}$$

with

$$f(X) = 4X^3 - 4(\theta - \theta^2)X^2 + 4(1 - \theta - \theta^3)X, \quad g(X) = (X^2 - (1 - \theta - \theta^3))^2.$$

At ∞_1,

$$\epsilon_{\infty_1}^{-1} = \inf_{(X,Y)\in E(\mathbf{R})} \frac{\max(|f(X)|, |g(X)|)}{\max(1, |X|)^4},$$

with infimum taken over $X \in \mathbb{R}$ such that $f(X) \ge 0$, that is, over $[0, \infty)$. This infimum occurs at the root 0.023441018652769... of $f(X) - g(X) = 0$, and has value 0.00796927528986859148..., so that

$$\boxed{\epsilon_{\infty_1} = 125.48192446950711297112...}.$$

At ∞_2,

$$\epsilon_{\infty_2}^{-1} = \inf_{(X,Y)\in E(\mathbf{R})} \frac{\max(|\bar{f}(X)|, |\bar{g}(X)|)}{\max(1,|X|)^4},$$

where

$$\bar{f}(X) = 4X^3 + 4(\theta+\theta^2)X^2 + 4(1+\theta+\theta^3)X, \quad \bar{g}(X) = (X^2 - (1+\theta+\theta^3))^2,$$

with infimum taken over $X \in \mathbf{R}$ such that $f(X) \geq 0$, that is, over $[0,\infty)$. This infimum occurs at the root 5.645614058038130... of $\bar{f}(X) - \bar{g}(X) = 0$, and has value 0.88372963806597132831... so that

$$\boxed{\epsilon_{\infty_2} = 1.13156779735087822111...}.$$

At ∞_3,

$$\epsilon_{\infty_3}^{-1} = \inf_{(X,Y)\in E(\mathbf{C})} \frac{\max(|F(X)|, |G(X)|)}{\max(1,|X|)^4},$$

where

$$F(X)^2 = 16X^2(X^4 - (4+2\theta^2)X^3 + (9+3\theta^2)X^2 - (10+4\theta^2)X + (5+2\theta^2)),$$

$$G(X) = (X^4 - 2X^2 + (5+2\theta^2)).$$

The infimum occurs at the root $1.455086138050493956497..-0.544920079668930802096...i$ of $|F(z)| = |G(z)|$, with value 0.67959006502634452483776 98... (on the unit circle, the minimum taken exceeds 4). Thus

$$\boxed{\epsilon_{\infty_3} = 1.47147530763451446602571 7...}$$

Putting the above together results in

$$\begin{aligned} h(P) - 2\hat{h}(P) \quad \leq \quad & \frac{1}{4}(\frac{1}{3}\cdot 1 \cdot \log(125.48192446950711297112) \\ & + \frac{1}{3}\cdot 1 \cdot \log(1.13156779735087822111) \\ & + \frac{1}{3}\cdot 2 \cdot \log(1.47147530763451446602571 7)), \end{aligned}$$

that is,

$$h(P) - 2\hat{h}(P) \leq 0.477358069897830...$$

Suppose now the point G_2 at (11) is not a generator. We easily check that G_2 is not divisible by 2 in $E(K)$, and so $G_2 = mQ$ for $m \geq 3$ and $Q \in E(K)$. Note that since $(1+\theta)^2 x(G_2) \in \mathcal{O}_K$, it follows that $(1+\theta)^2 x(Q) \in \mathcal{O}_K$. Then

$$h(Q) \leq 0.47735806989783 + 2\hat{h}(Q) < 0.47735806989783 + 2 * \hat{h}(G_2)/m^2 < 0.533699$$

so that

$$H(Q) < 1.70523.$$

Arguing as in the previous instance, we have to consider all polynomials of type
• $X^4 + 4c_1X^3 + 2c_2X^2 + 4c_3X + c_4$, $c_i \in \mathbb{Z}$, $|c_1| \leq 1$, $|c_2| \leq 8$, $|c_3| \leq 4$, $|c_4| \leq 8$

• $X^2 + 2c_1X + c_2$, $c_i \in \mathbb{Z}$, $|c_1| \leq 1$, $|c_2| \leq 2$
• $X + c_1$, $c_1 \in \mathbb{Z}$, $|c_1| \leq 1$
and
• $X^4 + 4c_1X^3 + c_2X^2 + 2c_3X + \frac{c_4}{4}$, $c_i \in \mathbb{Z}$, $c_2 \equiv c_4 \equiv 1 \pmod 2$, $|c_1| \leq 1$, $|c_2| \leq 17$, $|c_3| \leq 9$, $|c_4| \leq 33$
• $X^2 + 2c_1X + \frac{c_2}{4}$, $c_i \in \mathbb{Z}$, $c_2 \equiv 3 \pmod 4$, $|c_1| \leq 1$, $|c_2| < 11$.
Each polynomial has to be tested to see if a root can be the X-coordinate of a point in $\mathcal{E}_2(K)$. Computation shows that in the given range, only the points $\pm G_2$, $\pm G_2 + (0,0)$ arise. It follows that G_2 is indeed a generator of the group of points defined over K.

5.3 The curve $\mathcal{E}_3$ at (13)

¿From the table of Kodaira reduction types, we have $\mu_\nu = 0$ except for

$$\boxed{\mu_{\infty_1} = \mu_{\infty_2} = \mu_{\infty_3} = \tfrac{1}{3}.}$$

Further,

$$\epsilon_\nu^{-1} = \inf_{(X,Y)\in E(K_\nu)} \frac{\max(|f(X)|_\nu, |g(X)|_\nu)}{\max(1, |X|_\nu)^4}$$

with

$$f(X) = 4X^3 - 4(1+\theta)X^2 + 4(\theta + \theta^2 - \theta^3)X, \quad g(X) = (X^2 - (\theta + \theta^2 - \theta^3))^2.$$

At ∞_1,

$$\epsilon_{\infty_1}^{-1} = \inf_{(X,Y)\in E(\mathbf{R})} \frac{\max(|f(X)|, |g(X)|)}{\max(1, |X|)^4},$$

and the infimum needs to be taken over $X \in \mathbf{R}$ such that $f(X) \geq 0$, that is, over $[0, \infty)$. This infimum occurs at the turning point 0.738691905746190... of $f(X)0$, and has value 0.36278136846310610700..., so that

$$\boxed{\epsilon_{\infty_1} = 2.756481139691431866 36...}.$$

At ∞_2,

$$\epsilon_{\infty_2}^{-1} = \inf_{(X,Y)\in E(\mathbf{R})} \frac{\max(|\bar{f}(X)|, |\bar{g}(X)|)}{\max(1, |X|)^4},$$

where

$$\bar{f}(X) = 4X^3 - 4(1-\theta)X^2 + 4(-\theta + \theta^2 + \theta^3)X, \quad \bar{g}(X) = (X^2 - (-\theta + \theta^2 + \theta^3))^2,$$

with infimum taken over $X \in \mathbf{R}$ such that $f(X) \geq 0$, that is, over $[0, \infty)$. This infimum occurs at the root 0.010221121380833... of $\bar{f}(X) - \bar{g}(X) = 0$, and has value 0.00137643273231028235... so that

$$\boxed{\epsilon_{\infty_2} = 726.51570725257570965658...}.$$

At ∞_3,

$$\epsilon_{\infty_3}^{-1} = \inf_{(X,Y)\in E(\mathbf{C})} \frac{\max(|F(X)|, |G(X)|)}{\max(1, |X|)^4},$$

where

$$F(X)^2 = 16X^2(X^4 - 2X^3 - (1+\theta^2)X^2 - (10+4\theta^2)X + (29+12\theta^2)),$$

$$G(X) = (X^4 - 2X^2 + (5+2\theta^2)).$$

The infimum occurs at the root $-1.373429635060485748 88...-1.985476809807611687126...i$ of $|F(z)| = |G(z)|$, with value 0.12298493397299549431361611 49... (on the unit circle, the minimum taken exceeds 24). Thus

$$\boxed{\epsilon_{\infty_3} = 8.131077260403097196563785 12...}$$

Putting the above together results in

$$\begin{aligned} h(P) - 2\hat{h}(P) \quad \leq \quad & \frac{1}{4}(\frac{1}{3}\cdot 1 \cdot \log(2.75648113969143186636) \\ & + \frac{1}{3}\cdot 1 \cdot \log(726.51570725257570965658) \\ & + \frac{1}{3}\cdot 2 \cdot \log(8.131077260403097196563785 12)), \end{aligned}$$

that is,

$$h(P) - 2\hat{h}(P) \leq 0.982800154866326...$$

Suppose now the point G_3 at (14) is not a generator. We easily check that G_3 is not divisible by 2 in $E(K)$, and so $G_3 = mQ$ for $m \geq 3$ and $Q \in E(K)$. Note that since $(1+\theta)^2 x(G_3) \in \mathcal{O}_K$, it follows that $(1+\theta)^2 x(Q) \in \mathcal{O}_K$. Then

$$h(Q) \leq 0.982800154866326 + 2\hat{h}(Q) < 0.982800154866326 + 2\hat{h}(G_3)/m^2 < 1.037355$$

so that

$$H(Q) < 2.82175.$$

Arguing as in the previous instance, we have to consider all polynomials of type
• $X^4 + 4c_1X^3 + 2c_2X^2 + 4c_3X + c_4$, $c_i \in \mathbb{Z}$, $|c_1| \leq 2$, $|c_2| \leq 23$, $|c_3| \leq 22$, $|c_4| \leq 63$
• $X^2 + 2c_1X + c_2$, $c_i \in \mathbb{Z}$, $|c_1| \leq 2$, $|c_2| \leq 7$
• $X + c_1$, $c_1 \in \mathbb{Z}$, $|c_1| \leq 2$
and
• $X^4 + 4c_1X^3 + c_2X^2 + 2c_3X + \frac{c_4}{4}$, $c_i \in \mathbb{Z}$, $c_2 \equiv c_4 \equiv 1 \pmod 2$, $|c_1| \leq 2$, $|c_2| \leq 47$, $|c_3| \leq 44$, $|c_4| \leq 253$
• $X^2 + 2c_1X + \frac{c_2}{4}$, $c_i \in \mathbb{Z}$, $c_2 \equiv 3 \pmod 4$, $|c_1| \leq 2$, $|c_2| < 31$.
Each polynomial has to be tested to see if a root can be the X-coordinate of a point in $\mathcal{E}_3(K)$. Computation shows that in the given range, only the points $\pm G_3$, $\pm G_3 + (0,0)$ arise. It follows that G_3 is indeed a generator of the group of points defined over K.

5.4 The curve $\mathcal{E}_4$ at (15)

¿From the table of Kodaira reduction types, we have $\mu_\nu = 0$ except for

$$\boxed{\mu_{\infty_1} = \mu_{\infty_2} = \mu_{\infty_3} = \tfrac{1}{3}.}$$

Further,

$$\epsilon_\nu^{-1} = \inf_{(X,Y)\in E(K_\nu)} \frac{\max(|f(X)|_\nu, |g(X)|_\nu)}{\max(1,|X|_\nu)^4}$$

with

$$f(X) = 4X^3 - 4(1-\theta)X^2 + 4(-\theta+\theta^2+\theta^3)X, \quad g(X) = (X^2 - (-\theta+\theta^2+\theta^3))^2.$$

The curve is the conjugate of the curve (13) under $\theta \to -\theta$, and so

$$\boxed{\epsilon_{\infty_1} = 726.51570725257570965658...},$$

$$\boxed{\epsilon_{\infty_2} = 2.75648113969143186636...}$$

At ∞_3,

$$\epsilon_{\infty_3}^{-1} = \inf_{(X,Y)\in E(\mathbf{C})} \frac{\max(|F(X)|, |G(X)|)}{\max(1,|X|)^4},$$

where

$$F(X)^2 = 16X^2(X^4 - 2X^3 - (1+\theta^2)X^2 - (10+4\theta^2)X + (29+12\theta^2)),$$

$$G(X) = (X^4 - 2X^2 + (5+2\theta^2)).$$

The infimum occurs at the root $-1.37342963506048574888049...-1.985476809807611687126...i$ of $|F(z)| = |G(z)|$, with value 0.12298493397299549431361611 49... (on the unit circle, the minimum taken exceeds 24). Thus

$$\boxed{\epsilon_{\infty_3} = 8.13107726040309719656378512...}$$

Putting the above together results in

$$\begin{aligned} h(P) - 2\hat{h}(P) \quad \leq \quad & \frac{1}{4}(\frac{1}{3}\cdot 1\cdot \log(726.51570725257570965658) \\ & + \frac{1}{3}\cdot 1\cdot \log(2.75648113969143186636) \\ & + \frac{1}{3}\cdot 2\cdot \log(8.13107726040309719656378512)), \end{aligned}$$

that is,

$$h(P) - 2\hat{h}(P) \leq 0.982800154866326...$$

Suppose now the point G_4 at (16) is not a generator. We easily check that G_4 is not divisible by 2 in $E(K)$, and so $G_4 = mQ$ for $m \geq 3$ and $Q \in E(K)$. Note that since $(1+\theta)^2 x(G_4) \in \mathcal{O}_K$, it follows that $(1+\theta)^2 x(Q) \in \mathcal{O}_K$. Then

$$h(Q) \leq 0.982800154866326 + 2\hat{h}(Q) < 0.982800154866326 + 2\hat{h}(G_4)/m^2 < 1.037355$$

so that

$$H(Q) < 2.82175.$$

Arguing as in the previous instance, we have to consider all polynomials of type
• $X^4 + 4c_1X^3 + 2c_2X^2 + 4c_3X + c_4$, $c_i \in \mathbb{Z}$, $|c_1| \leq 2$, $|c_2| \leq 23$, $|c_3| \leq 22$, $|c_4| \leq 63$

• $X^2 + 2c_1X + c_2$, $c_i \in \mathbb{Z}$, $|c_1| \le 2$, $|c_2| \le 7$
• $X + c_1$, $c_1 \in \mathbb{Z}$, $|c_1| \le 2$
and
• $X^4 + 4c_1X^3 + c_2X^2 + 2c_3X + \frac{c_4}{4}$, $c_i \in \mathbb{Z}$, $c_2 \equiv c_4 \equiv 1 \pmod 2$, $|c_1| \le 2$, $|c_2| \le 47$, $|c_3| \le 44$, $|c_4| \le 253$
• $X^2 + 2c_1X + \frac{c_2}{4}$, $c_i \in \mathbb{Z}$, $c_2 \equiv 3 \pmod 4$, $|c_1| \le 2$, $|c_2| < 31$.
Each polynomial has to be tested to see if a root can be the X-coordinate of a point in $\mathcal{E}_4(K)$. Computation shows that in the given range, only the points G_4, $\pm G_4 + (0,0)$ arise. It follows that G_4 is indeed a generator of the group of points defined over K.

5.5 The curve $\mathcal{E}_5$ at (18)

¿From the table of Kodaira reductions, we have $\mu_\nu = 0$ except for

$$\boxed{\mu_\pi = \tfrac{1}{4}, \qquad \mu_{\infty_1} = \mu_{\infty_2} = \mu_{\infty_3} = \tfrac{1}{3}.}$$

Further,

$$\epsilon_\nu^{-1} = \inf_{(X,Y)\in E(K_\nu)} \frac{\max(|f(X)|_\nu, |g(X)|_\nu)}{\max(1, |X|_\nu)^4}$$

with

$$f(X) = 4X^3 - 4\phi X^2 + (4 + 2\phi^2)X, \quad g(X) = (X^2 - (1 + \phi^2/2))^2.$$

Siksek gives a method for computing the ϵ_ν. For the non-Archimedean valuation, we have the following (in Siksek's notation). First, we observe that $g(1 - \frac{1}{2}\phi + \frac{1}{4}\phi^3) \equiv 0 \pmod{\pi^{10}}$, and $g(X) \not\equiv 0 \pmod{\pi^{12}}$ for any $X \in K$. Thus $\epsilon_\pi = |\pi|_\pi^{-2j} = (2^{-\frac{1}{4}})^{-2j}$, where $j \le 5$. This weak inequality is all that we need, resulting in

$$\boxed{\epsilon_\pi \le 2^{\frac{5}{2}}}.$$

At ∞_1,

$$\epsilon_{\infty_1}^{-1} = \inf_{(X,Y)\in E(\mathbf{R})} \frac{\max(|f(X)|, |g(X)|)}{\max(1, |X|)^4},$$

and the infimum needs to be taken over $X \in \mathbf{R}$ such that $f(X) \ge 0$, that is, over $[0, \infty)$. This infimum occurs at the 4.108570541436509... of $f(X) = g(X)$, and has value 0.839461511264944344 91..., so that

$$\boxed{\epsilon_{\infty_1} = 1.19123984432966783131...}.$$

At ∞_2,

$$\epsilon_{\infty_2}^{-1} = \inf_{(X,Y)\in E(\mathbf{R})} \frac{\max(|\bar{f}(X)|, |\bar{g}(X)|)}{\max(1, |X|)^4},$$

where

$$\bar{f}(X) = 4X^3 + 4\phi X^2 + (4 + 2\phi^2)X, \quad \bar{g}(X) = (X^2 - (1 + \phi^2/2))^2,$$

with infimum taken over $X \in \mathbf{R}$ such that $f(X) \geq 0$, that is, over $[0, \infty)$. This infimum occurs at the root 5.383909674320621... of $\bar{f}(X) - \bar{g}(X) = 0$, and has value 0.90480288995171512682... so that

$$\boxed{\epsilon_{\infty_2} = 1.10521309238232547422...}.$$

At ∞_3,

$$\epsilon_{\infty_3}^{-1} = \inf_{(X,Y)\in E(\mathbf{C})} \frac{\max(|F(X)|, |G(X)|)}{\max(1, |X|)^4},$$

where

$$F(X)^2 = 16X^2(X^4 + 2X^2 + 2),$$
$$G(X) = X^4 + (2 + \phi^2)X^2 + 2.$$

The infimum occurs at the root $-0.444261439847776944198...-1.10310712781555133813262 1...i$ of $|F(z)| = |G(z)|$, with value 0.55824164662776903416988 09... (on the unit circle, the minimum taken exceeds 2). Thus

$$\boxed{\epsilon_{\infty_3} = 1.79133894083468807205636 3...}$$

Putting the above together results in

$$\begin{aligned} h(P) - 2\hat{h}(P) \quad \leq \quad & \frac{1}{4}(\frac{1}{4} \cdot 4 \cdot \log 2^{\frac{5}{2}} + \frac{1}{3} \cdot 1 \cdot \log(1.19123984432966783131) \\ & + \frac{1}{3} \cdot 1 \cdot \log(1.10521309238232547422) \\ & + \frac{1}{3} \cdot 2 \cdot \log(1.79133894083468807205636 3)), \end{aligned}$$

that is,

$$h(P) - 2\hat{h}(P) \leq 0.553296947402687...$$

Suppose now the point G_5 at (19) is not a generator. We easily check that G_5 is not divisible by 2 in $E(K)$, and so $G_5 = mQ$ for $m \geq 3$ and $Q \in E(K)$, with $x(Q) \in \mathcal{O}_K$. Then

$$h(Q) \leq 0.553296947402687 + 2\hat{h}(Q) < 0.553296947402687 + 2\hat{h}(G_5)/m^2 < 0.609176$$

so that

$$H(Q) < 1.83892.$$

Write $H(Q) < B$. By direct computation, if $|\mathbb{Q}(x(Q)) : \mathbb{Q}| = 4$, then the minimal polynomial for x(Q) is of type $X^4 + 4a_1X^3 + 2a_2X^2 + 4a_3X + a_4$, with $a_i \in \mathbb{Z}$, and, from (45), $|a_1| < B$, $|a_2| < 3B^2$, $|a_3| < B^3$, $|a_4| < B^4$. Similarly, if $|\mathbb{Q}(x(Q)) : \mathbb{Q}| = 2$, then the minimal polynomial of $x(Q)$ is of type $X^2 + 2a_1X + a_2$, $a_i \in Z$, with, from (46), $|a_1| < B$, $|a_2| < B^2$. Accordingly, we have to consider polynomials of the following types, where $a_i \in \mathbb{Z}$:

$$\begin{aligned} x^4 + 4a_1x^3 + 2a_2x^2 + 4a_3x + a_4, \quad & |a_1| \leq 1, |a_2| \leq 10, |a_3| \leq 6, |a_4| \leq 11, \\ x^2 + 2a_1x + a_2, \quad & |a_1| \leq 1, |a_2| \leq 3, \\ x + a_1, \quad & |a_1| \leq 1. \end{aligned}$$

Each polynomial has to be tested to see if a root can be the X-coordinate of a point in $\mathcal{E}_5(K)$. Computation shows that in the given range, only the points $\pm G_5$, $\pm G_5 + (0, 0)$ arise. It follows that G_5 is indeed a generator of the group of points defined over K.

5.6 The curve $\mathcal{E}_6$ at (20)

¿From the table of Kodaira reductions, we have $\mu_\nu = 0$ except for

$$\boxed{\mu_\pi = \tfrac{1}{4}, \qquad \mu_{\infty_1} = \mu_{\infty_2} = \mu_{\infty_3} = \tfrac{1}{3}.}$$

Further,

$$\epsilon_\nu^{-1} = \inf_{(X,Y)\in E(K_\nu)} \frac{\max(|f(X)|_\nu, |g(X)|_\nu)}{\max(1,|X|_\nu)^4}$$

with

$$f(X) = 4X^3 + (-4+2\phi^2)X^2 + (4-2\phi^2)X, \quad g(X) = (X^2 - (1-\phi^2/2))^2.$$

Siksek gives a method for computing the ϵ_ν. For the non-Archimedean valuation, we have the following (in Siksek's notation). First, we observe that $g(1-\frac{1}{2}\phi-\frac{1}{4}\phi^3) \equiv 0 \pmod{\pi^{10}}$, and $g(X) \not\equiv 0 \pmod{\pi^{12}}$ for any $X \in K$. Thus $\epsilon_\pi = |\pi|_\pi^{-2j} = (2^{-\frac{1}{4}})^{-2j}$, where $j \le 5$. This weak inequality is all that we need, resulting in

$$\boxed{\epsilon_\pi \le 2^{\frac{5}{2}}}.$$

At ∞_1,

$$\epsilon_{\infty_1}^{-1} = \inf_{(X,Y)\in E(\mathbf{R})} \frac{\max(|f(X)|, |g(X)|)}{\max(1,|X|)^4},$$

and the infimum needs to be taken over $X \in \mathbf{R}$ such that $f(X) \ge 0$, that is, over $[0,\infty)$. This infimum occurs at the root 0.152240934977426... of $f(X) = g(X)$, and has value 0.31652903917264027803..., so that

$$\boxed{\epsilon_{\infty_1} = 3.15926779613602254445...}.$$

At ∞_2, the curve is invariant under $\phi \to -\phi$, and so

$$\boxed{\epsilon_{\infty_2} = 3.15926779613602254445...}.$$

At ∞_3,

$$\epsilon_{\infty_3}^{-1} = \inf_{(X,Y)\in E(\mathbf{C})} \frac{\max(|F(X)|, |G(X)|)}{\max(1,|X|)^4},$$

where

$$F(X)^2 = 16X^2(X^4 - (6+\phi^2)X^3 + (16+3\phi^2)X^2 - (20+4\phi^2)X + (10+2\phi^2)),$$

$$G(X) = X^4 - (6+\phi^2)X^2 + (10+2\phi^2).$$

The infimum occurs at the root $1.797932651931813404063... - 0.426206219441401112133512...i$ of $|F(z)| = |G(z)|$, with value 0.21281825307292408932846977 5... (on the unit circle, the minimum taken exceeds 4). Thus

$$\boxed{\epsilon_{\infty_3} = 4.69884507348785069728174 04...}$$

Putting the above together results in

$$\begin{aligned} h(P) - 2\hat{h}(P) &\leq \frac{1}{4}(\frac{1}{4}\cdot 4\cdot \log 2^{\frac{5}{2}} + \frac{1}{3}\cdot 1\cdot \log(3.15926779613602254445) \\ &\quad + \frac{1}{3}\cdot 1\cdot \log(3.15926779613602254445) \\ &\quad + \frac{1}{3}\cdot 2\cdot \log(4.69884507348785069)), \end{aligned}$$

that is,

$$h(P) - 2\hat{h}(P) \leq 0.882826494540115...$$

Suppose now the point G_6 at (21) is not a generator. We easily check that G_6 is not divisible by 2 in $E(K)$, and so $G_6 = mQ$ for $m \geq 3$ and $Q \in E(K)$, with $x(Q) \in \mathcal{O}_K$. Then

$$h(Q) \leq 0.882826494540115 + 2\hat{h}(Q) < 0.882826494540115 + 2\hat{h}(G_6)/m^2 < 0.923750$$

so that

$$H(Q) < 2.51872.$$

Arguing as in the case of the curve (18), we must consider polynomials of the following types, where $a_i \in \mathbb{Z}$:

$$\begin{aligned} x^4 + 4a_1x^3 + 2a_2x^2 + 4a_3x + a_4, &\quad |a_1| \leq 2, |a_2| \leq 19, |a_3| \leq 15, |a_4| \leq 40, \\ x^2 + 2a_1x + a_2, &\quad |a_1| \leq 2, |a_2| \leq 6, \\ x + a_1, &\quad |a_1| \leq 2. \end{aligned}$$

Each polynomial has to be tested to see if a root can be the X-coordinate of a point in $\mathcal{E}_6(K)$. Computation shows that in the given range, only the points $\pm G_6$, $\pm G_6 + (0,0)$ arise. It follows that G_6 is indeed a generator of the group of points defined over K.

5.7 The curve $\mathcal{E}_7$ at (22)

¿From the table of Kodaira reductions, we have $\mu_\nu = 0$ except for

$$\boxed{\mu_\pi = \tfrac{1}{4}, \qquad \mu_{\infty_1} = \mu_{\infty_2} = \mu_{\infty_3} = \tfrac{1}{3}.}$$

Further,

$$\epsilon_\nu^{-1} = \inf_{(X,Y)\in E(K_\nu)} \frac{\max(|f(X)|_\nu, |g(X)|_\nu)}{\max(1, |X|_\nu)^4}$$

with

$$\begin{aligned} f(X) &= 4X^3 + (-8 - 8\phi - 2\phi^3)X^2 + (52 + 56\phi + 10\phi^2 + 12\phi^3)X, \\ g(X) &= (X^2 - (13 + 14\phi + \frac{5}{2}\phi^2 + 3\phi^3))^2. \end{aligned}$$

Siksek gives a method for computing the ϵ_ν. For the non-Archimedean valuation, we have the following (in Siksek's notation). First, we observe that $g(1 + \frac{1}{2}\phi - \frac{1}{4}\phi^3) \equiv 0$

(mod π^{10}), and $g(X) \not\equiv 0 \pmod{\pi^{12}}$ for any $X \in K$. Thus $\epsilon_\pi = |\pi|_\pi^{-2j} = (2^{-\frac{1}{4}})^{-2j}$, where $j \leq 5$. This weak inequality is all that we need, resulting in

$$\boxed{\epsilon_\pi \leq 2^{\frac{5}{2}}}.$$

At ∞_1,

$$\epsilon_{\infty_1}^{-1} = \inf_{(X,Y)\in E(\mathbf{R})} \frac{\max(|f(X)|, |g(X)|)}{\max(1, |X|)^4},$$

and the infimum needs to be taken over $X \in \mathbf{R}$ such that $f(X) \geq 0$, that is, over $[0, \infty)$. This infimum occurs at the root 9.043006133337668... of $f(X) = g(X)$, and has value 0.39970098305719519573..., so that

$$\boxed{\epsilon_{\infty_1} = 2.50187025398660338324...}.$$

At ∞_2,

$$\epsilon_{\infty_2}^{-1} = \inf_{(X,Y)\in E(\mathbf{R})} \frac{\max(|\bar{f}(X)|, |\bar{g}(X)|)}{\max(1, |X|)^4},$$

where

$$\begin{aligned} \bar{f}(X) &= 4X^3 + (-8 + 8\phi + 2\phi^3)\phi X^2 + (52 - 56\phi + 10\phi^2 - 12\phi^3)X, \\ \bar{g}(X) &= (X^2 - (13 - 14\phi + \frac{5}{2}\phi^2 - 3\phi^3))^2, \end{aligned}$$

with infimum taken over $X \in \mathbf{R}$ such that $f(X) \geq 0$, that is, over $[0, \infty)$. This infimum occurs at the root 0.015710679827598... of $\bar{f}(X) - \bar{g}(X) = 0$, and has value 0.00438935169160511858... so that

$$\boxed{\epsilon_{\infty_2} = 227.82407750842934587031...}.$$

At ∞_3,

$$\epsilon_{\infty_3}^{-1} = \inf_{(X,Y)\in E(\mathbf{C})} \frac{\max(|F(X)|, |G(X)|)}{\max(1, |X|)^4},$$

where

$$F(X)^2 = 16X^2(X^4 - 4X^3 + (10 - 4\phi^2)X^2 - (4 + 2\phi^2)X + 2),$$
$$G(X) = X^4 + (-6 + 5\phi^2)X^2 + 2.$$

The infimum occurs at the root 1.164435178539534874799...$-$0.241462786682951600036697...i of $|F(z)| = |G(z)|$, with value 0.52138210146214758954528399... (on the unit circle, the minimum taken exceeds 0.90). Thus

$$\boxed{\epsilon_{\infty_3} = 1.91797915040741024372277 73...}$$

Putting the above together results in

$$\begin{aligned} h(P) - 2\hat{h}(P) \leq\ & \frac{1}{4}(\frac{1}{4} \cdot 4 \cdot \log 2^{\frac{5}{2}} + \frac{1}{3} \cdot 1 \cdot \log(2.50187025398660338324) \\ & + \frac{1}{3} \cdot 1 \cdot \log(227.82407750842934587031) \\ & + \frac{1}{3} \cdot 2 \cdot \log(1.917979150407410243722)), \end{aligned}$$

that is,

$$h(P) - 2\hat{h}(P) \leq 1.070563363421848...$$

Suppose now the point G_7 at (23) is not a generator. We easily check that G_7 is not divisible by 2 in $E(K)$, and so $G_7 = mQ$ for $m \geq 3$ and $Q \in E(K)$, with $x(Q) \in \mathcal{O}_K$. Then

$$h(Q) \leq 1.070563363421848 + 2\hat{h}(Q) < 1.070563363421848 + 2\hat{h}(G_7)/m^2 < 1.095543$$

so that

$$H(Q) < 2.99081.$$

Arguing as in the case of the curve (18), we must consider polynomials of the following types, where $a_i \in \mathbb{Z}$:

$$\begin{array}{rl} x^4 + 4a_1x^3 + 2a_2x^2 + 4a_3x + a_4, & |a_1| \leq 2, |a_2| \leq 26, |a_3| \leq 26, |a_4| \leq 80, \\ x^2 + 2a_1x + a_2, & |a_1| \leq 2, |a_2| \leq 8, \\ x + a_1, & |a_1| \leq 2. \end{array}$$

Each polynomial has to be tested to see if a root can be the X-coordinate of a point in $\mathcal{E}_7(K)$. Computation shows that in the given range, only the points $\pm G_7$ arise. It follows that G_7 is indeed a generator of the group of points defined over K.

5.8 The curve $\mathcal{E}_8$ at (24)

¿From the table of Kodaira reductions, we have $\mu_\nu = 0$ except for

$$\boxed{\mu_\pi = \tfrac{1}{4}, \qquad \mu_{\infty_1} = \mu_{\infty_2} = \mu_{\infty_3} = \tfrac{1}{3}.}$$

Further,

$$\epsilon_\nu^{-1} = \inf_{(X,Y) \in E(K_\nu)} \frac{\max(|f(X)|_\nu, |g(X)|_\nu)}{\max(1, |X|_\nu)^4}$$

with

$$\begin{aligned} f(X) &= 4X^3 + (-4 - 4\phi - 2\phi^2 - 2\phi^3)X^2 + (20 + 24\phi + 6\phi^2 + 4\phi^3)X, \\ g(X) &= (X^2 - (5 + 6\phi + \frac{3}{2}\phi^2 + \phi^3))^2. \end{aligned}$$

Siksek gives a method for computing the ϵ_ν. For the non-Archimedean valuation, we have the following (in Siksek's notation).

First, we observe that $g(1 + \frac{1}{2}\phi + \frac{1}{4}\phi^3) \equiv 0 \pmod{\pi^{10}}$, and $g(X) \not\equiv 0 \pmod{\pi^{12}}$ for any $X \in K$. Thus $\epsilon_\pi = |\pi|_\pi^{-2j} = (2^{-\frac{1}{4}})^{-2j}$, where $j \leq 5$. This weak inequality is all that we need, resulting in

$$\boxed{\epsilon_\pi \leq 2^{\frac{5}{2}}}.$$

At ∞_1,

$$\epsilon_{\infty_1}^{-1} = \inf_{(X,Y) \in E(\mathbf{R})} \frac{\max(|f(X)|, |g(X)|)}{\max(1, |X|)^4},$$

and the infimum needs to be taken over $X \in \mathbf{R}$ such that $f(X) \geq 0$, that is, over $[0, \infty)$. This infimum occurs at the root 6.700009106939032... of $f(X) = g(X)$, and has value 0.52198282519734460776..., so that

$$\boxed{\epsilon_{\infty_1} = 1.91577184483403789523...}.$$

At ∞_2,

$$\epsilon_{\infty_2}^{-1} = \inf_{(X,Y)\in E(\mathbf{R})} \frac{\max(|\bar{f}(X)|, |\bar{g}(X)|)}{\max(1, |X|)^4},$$

where

$$\begin{aligned} \bar{f}(X) &= 4X^3 + (-4 + 4\phi - 2\phi^2 + 2\phi^3)X^2 + (20 - 24\phi + 6\phi^2 - 4\phi^3)X, \\ \bar{g}(X) &= (X^2 - (5 - 6\phi + \frac{3}{2}\phi^2 - \phi^3))^2, \end{aligned}$$

with infimum taken over $X \in \mathbf{R}$ such that $f(X) \geq 0$, that is, over $[0, \infty)$. This infimum occurs at the root 0.007079403590926... of $\bar{f}(X) - \bar{g}(X) = 0$, and has value 0.00075595704579275884... so that

$$\boxed{\epsilon_{\infty_2} = 1322.82648275513803837226...}.$$

At ∞_3,

$$\epsilon_{\infty_3}^{-1} = \inf_{(X,Y)\in E(\mathbf{C})} \frac{\max(|F(X)|, |G(X)|)}{\max(1, |X|)^4},$$

where

$$F(X)^2 = 16X^2(X^4 + (2 + \phi^2)X^3 + (8 - \phi^2)X^2 + (8 + 2\phi^2)X + (10 + 2\phi^2)),$$

$$G(X) = X^4 + (2 + 3\phi^2)X^2 + (10 + 2\phi^2).$$

The infimum occurs at the root $-0.12979371761754359839 6...-1.8431948223777410560...i$ of $|F(z)| = |G(z)|$, with value 0.66655470502960908650 4527189... (on the unit circle, the minimum taken exceeds 8). Thus

$$\boxed{\epsilon_{\infty_3} = 1.50025195599748847329235227...}$$

Putting the above together results in

$$\begin{aligned} h(P) - 2\hat{h}(P) \leq\ & \frac{1}{4}(\frac{1}{4} \cdot 4 \cdot \log 2^{\frac{5}{2}} + \frac{1}{3} \cdot 1 \cdot \log(1.91577184483403789523) \\ & + \frac{1}{3} \cdot 1 \cdot \log(1322.82648275513803837226) \\ & + \frac{1}{3} \cdot 2 \cdot \log(1.5002519559974884732923)), \end{aligned}$$

that is,

$$h(P) - 2\hat{h}(P) \leq 1.153959714852488...$$

Suppose now the point G_8 at (25) is not a generator. We easily check that G_8 is not divisible by 2 in $E(K)$, and so $G_8 = mQ$ for $m \geq 3$ and $Q \in E(K)$, with $x(Q) \in \mathcal{O}_K$. Then

$$h(Q) \leq 1.153959714852488 + 2\hat{h}(Q) < 1.153959714852488 + 2\hat{h}(G_8)/m^2 < 1.167799$$

so that

$$H(Q) < 3.21491.$$

Arguing as in the case of the curve (18), we must consider polynomials of the following types, where $a_i \in \mathbb{Z}$:

$$\begin{aligned} x^4 + 4a_1x^3 + 2a_2x^2 + 4a_3x + a_4, &\quad |a_1| \leq 3, |a_2| \leq 31, |a_3| \leq 33, |a_4| \leq 106, \\ x^2 + 2a_1x + a_2, &\quad |a_1| \leq 3, |a_2| \leq 10, \\ x + a_1, &\quad |a_1| \leq 3. \end{aligned}$$

Each polynomial has to be tested to see if a root can be the X-coordinate of a point in $\mathcal{E}_8(K)$. Computation shows that in the given range, only the points $\pm G_8$, $\pm G_8 + (0,0)$, $\pm 2G_8 + (0,0)$ arise. It follows that G_8 is indeed a generator of the group of points defined over K.

5.9 The curve $\mathcal{E}_9$ at (27)

¿From the table of Kodaira reductions, we have $\mu_\nu = 0$ except for

$$\boxed{\mu_\pi = \tfrac{1}{4}, \qquad \mu_{\infty_1} = \mu_{\infty_2} = \mu_{\infty_3} = \tfrac{1}{3}.}$$

Further,

$$\epsilon_\nu^{-1} = \inf_{(X,Y) \in E(K_\nu)} \frac{\max(|f(X)|_\nu, |g(X)|_\nu)}{\max(1, |X|_\nu)^4}$$

with

$$f(X) = 4X^3 + (-8\phi - 2\phi^3)X^2 + (4 + 2\phi^2)X, \quad g(X) = (X^2 - (1 + \phi^2/2))^2.$$

Siksek gives a method for computing the ϵ_ν. For the non-Archimedean valuation, we have the following (in Siksek's notation). First, we observe that $g(i1 + \frac{1}{2}\phi - \frac{1}{4}\phi^3) \equiv 0 \pmod{\pi^{10}}$, and $g(X) \not\equiv 0 \pmod{\pi^{12}}$ for any $X \in K$. Thus $\epsilon_\pi = |\pi|_\pi^{-2j} = (2^{-\frac{1}{4}})^{-2j}$, where $j \leq 5$. This weak inequality is all that we need, resulting in

$$\boxed{\epsilon_\pi \leq 2^{\frac{5}{2}}}.$$

At ∞_1,

$$\epsilon_{\infty_1}^{-1} = \inf_{(X,Y) \in E(\mathbf{R})} \frac{\max(|f(X)|, |g(X)|)}{\max(1, |X|)^4},$$

and the infimum needs to be taken over $X \in \mathbf{R}$ such that $f(X) \geq 0$, that is, over $[0, \infty)$. This infimum occurs at the root 1.432001362205440... of $g(X)$, and has value 0.43345064994236763769..., so that

$$\boxed{\epsilon_{\infty_1} = 2.30706771378232276809...}.$$

At ∞_2,

$$\epsilon_{\infty_2}^{-1} = \inf_{(X,Y)\in E(\mathbf{R})} \frac{\max(|\bar{f}(X)|, |\bar{g}(X)|)}{\max(1,|X|)^4},$$

where

$$\bar{f}(X) = 4X^3 + (8\phi + 2\phi^3)X^2 + (4 + 2\phi^2)X, \quad \bar{g}(X) = (X^2 - (1 + \phi^2/2))^2,$$

with infimum taken over $X \in \mathbf{R}$ such that $f(X) \geq 0$, that is, over $[0, \infty)$. This infimum occurs at the root 6.061612256558471... of $\bar{f}(X) - \bar{g}(X) = 0$, and has value 0.92450305111791316372... so that

$$\boxed{\epsilon_{\infty_2} = 1.08166219547982626230...}.$$

At ∞_3,

$$\epsilon_{\infty_3}^{-1} = \inf_{(X,Y)\in E(\mathbf{C})} \frac{\max(|F(X)|, |G(X)|)}{\max(1,|X|)^4},$$

where

$$F(X)^2 = 16X^2(X^4 - 2X^2 + 2)),$$
$$G(X) = X^4 + (2 + \phi^2)X^2 + 2.$$

The infimum occurs at the root $-4.75658463661294583777438 85...i$ of $|f(z)| = |g(z)|$, with value 0.87889423562779395918229 79... (on the unit circle, the minimum taken exceeds 4). Thus

$$\boxed{\epsilon_{\infty_3} = 1.13779333105501621587693 81...}$$

Putting the above together results in

$$\begin{aligned} h(P) - 2\hat{h}(P) \quad \leq \quad & \frac{1}{4}(\frac{1}{4} \cdot 4 \cdot \log 2^{\frac{5}{2}} + \frac{1}{3} \cdot 1 \cdot \log(2.30706771378232276809) \\ & + \frac{1}{3} \cdot 1 \cdot \log(1.08166219547982626230) \\ & + \frac{1}{3} \cdot 2 \cdot \log(1.13779333105501621587693 8)), \end{aligned}$$

that is,

$$h(P) - 2\hat{h}(P) \leq 0.530938461365339...$$

Suppose now the point G_9 at (28) is not a generator. We easily check that G_9 is not divisible by 2 in $E(K)$, and so $G_9 = mQ$ for $m \geq 3$ and $Q \in E(K)$, with $x(Q) \in \mathcal{O}_K$. Then

$$h(Q) \leq 0.530938461365339 + 2\hat{h}(Q) < 0.530938461365339 + 2\hat{h}(G_9)/m^2 < 0.558878$$

so that

$$H(Q) < 1.74871.$$

Arguing as in the case of the curve (18), we must consider polynomials of the following types, where $a_i \in \mathbb{Z}$:

$$\begin{aligned} x^4 + 4a_1x^3 + 2a_2x^2 + 4a_3x + a_4, \quad & |a_1| \leq 1, |a_2| \leq 9, |a_3| \leq 5, |a_4| \leq 9, \\ x^2 + 2a_1x + a_2, \quad & |a_1| \leq 1, |a_2| \leq 3, \\ x + a_1, \quad & |a_1| \leq 1. \end{aligned}$$

Each polynomial has to be tested to see if a root can be the X-coordinate of a point in $\mathcal{E}_9(K)$. Computation shows that in the given range, only the points $\pm G_9$, $\pm G_9 + (0,0)$, $\pm 2G_9 + (0,0)$ arise. It follows that G_9 is indeed a generator of the group of points defined over K.

5.10 The curve $\mathcal{E}_{10}$ at (29)

¿From the table of Kodaira reductions, we have $\mu_\nu = 0$ except for

$$\boxed{\mu_\pi = \tfrac{1}{4}, \qquad \mu_{\infty_1} = \mu_{\infty_2} = \mu_{\infty_3} = \tfrac{1}{3}.}$$

Further,

$$\epsilon_\nu^{-1} = \inf_{(X,Y)\in E(K_\nu)} \frac{\max(|f(X)|_\nu, |g(X)|_\nu)}{\max(1,|X|_\nu)^4}$$

with

$$f(X) = 4X^3 + (-4-2\phi^2)X^2 + (4-2\phi^2)X, \qquad g(X) = (X^2 - (1-\frac{1}{2}\phi^2))^2.$$

Siksek gives a method for computing the ϵ_ν. For the non-Archimedean valuation, we have the following (in Siksek's notation). At π, with $\nu(2) = 0$, then $\frac{1}{2}\phi + \frac{1}{2}\phi^2 - \frac{1}{4}\phi^3 \in U_5 \cap V_5$, and $U_6 = V_6 = \{\}$. Thus

$$\boxed{\epsilon_\pi = |\pi|_\pi^{-10} = (2^{-\frac{1}{4}})^{-10} = 2^{\frac{5}{2}}}.$$

At ∞_1,

$$\epsilon_{\infty_1}^{-1} = \inf_{(X,Y)\in E(\mathbf{R})} \frac{\max(|f(X)|, |g(X)|)}{\max(1,|X|)^4},$$

and the infimum needs to be taken over $X \in \mathbf{R}$ such that $f(X) \geq 0$, that is, over $[0,\infty)$. This infimum occurs at the turning point 0.635599759292601... of $f(X) = 0$, and has value 0.23110328892932097092..., so that

$$\boxed{\epsilon_{\infty_1} = 4.32706953082711459453...}$$

At ∞_2, since f and g are invariant under $\phi \to -\phi$, we have $\epsilon_{\infty_2} = \epsilon_{\infty_1}$.
At ∞_3,

$$\epsilon_{\infty_3}^{-1} = \inf_{(X,Y)\in E(\mathbf{C})} \frac{\max(|F(X)|, |G(X)|)}{\max(1,|X|)^4},$$

where

$$F(X)^2 = 16X^2(X^4 + (2+\phi^2)X^3 + (8+\phi^2)X^2 + (8+2\phi^2)X + (10+2\phi^2)),$$

$$G(X) = X^4 - (6+\phi^2)X^2 + (10+2\phi^2).$$

The infimum occurs at the root $-4.744484173612250054385189 6...$ of $|F(z)| = |G(z)|$, with value 0.71965609074895820190191934 13... (on the unit circle, the minimum taken exceeds 10). Thus

$$\boxed{\epsilon_{\infty_3} = 1.38955261110801296065795 2...}$$

Putting the above together results in

$$\begin{aligned} h(P) - 2\hat{h}(P) \quad \leq \quad & \frac{1}{4}(\frac{1}{4} \cdot 4 \cdot \log 2^{\frac{5}{2}} + \frac{1}{3} \cdot 1 \cdot \log(4.32706953082711459453) \\ & + \frac{1}{3} \cdot 1 \cdot \log(4.32706953082711459453) \\ & + \frac{1}{3} \cdot 2 \cdot \log(1.3895526111080129606)), \end{aligned}$$

that is,

$$h(P) - 2\hat{h}(P) \leq 0.732195715015999...$$

Suppose now that the points P_1 and P_2 at (30) and (31) do not generate the full group of points over K. We first check that that P_1 is not divisible in $E(K)$. It is easy to check that P_1 is not divisible by 2. Suppose $P_1 = mQ$ for $m \geq 3$, for $Q \in E(K)$, with $x(Q) \in \mathcal{O}_K$. Then

$$h(Q) \leq 2\hat{h}(Q) + 0.732195715015999 \leq 2/9\hat{h}(P_1) + 0.732195715015999 < 0.7532202040...,$$

so that

$$H(Q) < 2.12383.$$

If $|\mathbb{Q}(x(Q)) : \mathbb{Q}| = 4$, then from (45), $x(Q)$ is a root of a polynomial of type

$$x^4 + 4a_1x^3 + 2a_2x^2 + 4a_3x + a_4, \qquad |a_1| \leq 2, |a_2| \leq 13, |a_3| \leq 9, |a_4| \leq 20;$$

If $|\mathbb{Q}(x(Q)) : \mathbb{Q}| = 2$, then from (46), $X(Q)$ is a root of a polynomial of type

$$x^2 + 2a_1x + a_2, \qquad |a_1| \leq 2, |a_2| \leq 4;$$

and if $|\mathbb{Q}(x(Q)) : \mathbb{Q}| = 1$, then from (47), $x(Q)$ is a root of a polynomial of type

$$x + a_1, \qquad |a_1| \leq 2.$$

Search finds that the only points Q satisfying these inequalities are given by $\pm Q = P_1$, P_2, $P_1 + (0,0)$, $P_2 + (0,0)$, $P_1 \pm P_2$, $P_1 \pm P_2 + (0,0)$, $2P_1 + (0,0$, and $2P_2 + (0,0)$. Since P_1 and P_2 are of infinite order and independent, it follows that P_1 is not divisible. Further, it is straightforward to check that the index of the subgroup in $E(K)$ generated by P_1 and P_2 is *odd*. We take $P_1 = G_1$ as one of the generators of $E(K)$, and denote by G_2 a second generator. Put $P_2 = aG_1 + mG_2$, for $a, m \in \mathbb{Z}$, and where without loss of generality

$$m \geq 3, \qquad |a| < m/2. \tag{48}$$

It follows that

$$m^2\hat{h}(G_2) = \hat{h}(-aP_1 + P_2) = a^2\hat{h}(P_1) - a < P_1, P_2 > + \hat{h}(P_2) \tag{49}$$

so that

$$\hat{h}(G_2) = a^2/m^2\hat{h}(P_1) - a/m^2 < P_1, P_2 > + \hat{h}(P_2)/m^2,$$

whence using (48),

$$\hat{h}(G_2) < 1/4\hat{h}(P_1) + 1/6| < P_1, P_2 > | + \hat{h}(P_2)/9 < 0.035009546550940.$$

Thus

$$h(G_2) < 2\hat{h}(G_2) + 0.732195715015999 < 0.8022148081,$$

with

$$H(G_2) < 2.23048.$$

As above, $x(G_2)$ is a root of a polynomial of type
• $x^4 + 4a_1x^3 + 2a_2x^2 + 4a_3x + a_4, \qquad |a_1| \le 2, |a_2| \le 14, |a_3| \le 11, |a_4| \le 24$
• $x^2 + 2a_1x + a_2, \qquad |a_1| \le 2, |a_2| \le 4$
• $x + a_1, \qquad |a_1| \le 2.$
Search finds no points other than those found above in testing P_1 for divisibility, and it follows that indeed P_1 and P_2 generate the group of points over K.

5.11 The curve $\mathcal{E}_{11}$ at (33)

¿From the table of Kodaira reductions, we have $\mu_\nu = 0$ except for

$$\boxed{\mu_\pi = \tfrac{1}{4}, \qquad \mu_{\infty_1} = \mu_{\infty_2} = \mu_{\infty_3} = \tfrac{1}{3}.}$$

Further,

$$\epsilon_\nu^{-1} = \inf_{(X,Y)\in E(K_\nu)} \frac{\max(|f(X)|_\nu, |g(X)|_\nu)}{\max(1, |X|_\nu)^4}$$

with

$$\begin{aligned} f(X) &= 4X^3 + (-16 - 20\phi - 4\phi^2 - 4\phi^3)X^2 + (52 + 56\phi + 10\phi^2 + 12\phi^3)X, \\ g(X) &= (X^2 - (13 + 14\phi + \frac{5}{2}\phi^2 + 3\phi^3))^2. \end{aligned}$$

Siksek gives a method for computing the ϵ_ν. For the non-Archimedean valuation, we have the following (in Siksek's notation).

First, we observe that $g(1 - \frac{1}{2}\phi + \frac{1}{4}\phi^3) \equiv 0 \pmod{\pi^{10}}$, and $g(X) \not\equiv 0 \pmod{\pi^{12}}$ for any $X \in K$. Thus $\epsilon_\pi = |\pi|_\pi^{-2j} = (2^{-\frac{1}{4}})^{-2j}$, where $j \le 5$. This weak inequality is all that we need, resulting in

$$\boxed{\epsilon_\pi \le 2^{\frac{5}{2}}}.$$

At ∞_1,

$$\epsilon_{\infty_1}^{-1} = \inf_{(X,Y)\in E(\mathbf{R})} \frac{\max(|f(X)|, |g(X)|)}{\max(1, |X|)^4},$$

and the infimum needs to be taken over $X \in \mathbf{R}$ such that $f(X) \ge 0$, that is, over $[0, \infty)$. This infimum occurs at the root 6.585832771319615... of $f(X) = g(X)$, and has value 0.09399416728471314096..., so that

$$\boxed{\epsilon_{\infty_1} = 10.638958021415827273 14...}.$$

At ∞_2,

$$\epsilon_{\infty_2}^{-1} = \inf_{(X,Y)\in E(\mathbf{R})} \frac{\max(|\bar{f}(X)|, |\bar{g}(X)|)}{\max(1, |X|)^4},$$

where

$$\begin{aligned}\bar{f}(X) &= 4X^3 + (-16 + 20\phi - 4\phi^2 + 4\phi^3)X^2 + (52 - 56\phi + 10\phi^2 - 12\phi^3)X,\\ \bar{g}(X) &= (X^2 - (13 - 14\phi + \frac{5}{2}\phi^2 - 3\phi^3))^2,\end{aligned}$$

with infimum taken over $X \in \mathbf{R}$ such that $f(X) \geq 0$, that is, over $[0, \infty)$. This infimum occurs at the root 0.014878523374045... of $\bar{f}(X) - \bar{g}(X) = 0$, and has value 0.00439272523855358661... so that

$$\boxed{\epsilon_{\infty_2} = 227.64911204172531486370...}.$$

At ∞_3,

$$\epsilon_{\infty_3}^{-1} = \inf_{(X,Y)\in E(\mathbf{C})} \frac{\max(|F(X)|, |G(X)|)}{\max(1, |X|)^4},$$

where

$$F(X)^2 = 16X^2(X^4 + 2\phi^2 X^3 + (6 - 4\phi^2)X^2 + (4 - 2\phi^2)X + 2),$$
$$G(X) = X^4 + (-6 + 5\phi^2)X^2 + 2.$$

The infimum occurs at the root $-3.839123346088306...$ of $|F(z)| = |G(z)|$, with value 0.883154612846032931 03... (on the unit circle, the minimum taken 2.5). Thus

$$\boxed{\epsilon_{\infty_3} = 1.13230456530983167167...}$$

Putting the above together results in

$$\begin{aligned}h(P) - 2\hat{h}(P) \leq\ & \frac{1}{4}(\frac{1}{4}\cdot 4 \cdot \log 2^{\frac{5}{2}} + \frac{1}{3}\cdot 1 \cdot \log(10.638958021415827273 14)\\ & + \frac{1}{3}\cdot 1 \cdot \log(227.64911204172531486370)\\ & + \frac{1}{3}\cdot 2 \cdot \log(1.13230456530983167167)),\end{aligned}$$

that is,

$$h(P) - 2\hat{h}(P) \leq 1.103286821056004...$$

Suppose now the point G_{11} at (34) is not a generator. We easily check that G_{11} is not divisible by 2 in $E(K)$, and so $G_{11} = mQ$ for $m \geq 3$ and $Q \in E(K)$, with $x(Q) \in \mathcal{O}_K$. Then

$$h(Q) \leq 1.103286821056004 + 2\hat{h}(Q) < 1.103286821056004 + 2\hat{h}(G_{11})/m^2 < 1.153246$$

so that

$$H(Q) < 3.16847.$$

Arguing as in the case of the curve (18), we must consider polynomials of the following types, where $a_i \in \mathbb{Z}$:

$$\begin{aligned}x^4 + 4a_1x^3 + 2a_2x^2 + 4a_3x + a_4, &\quad |a_1| \leq 3, |a_2| \leq 30, |a_3| \leq 31, |a_4| \leq 100,\\ x^2 + 2a_1x + a_2, &\quad |a_1| \leq 3, |a_2| \leq 10,\\ x + a_1, &\quad |a_1| \leq 3.\end{aligned}$$

Each polynomial has to be tested to see if a root can be the X-coordinate of a point in $\mathcal{E}_{11}(K)$. Computation shows that in the given range, only the points $\pm G_{11}$, $\pm G_{11} + (0, 0)$ arise. It follows that G_{11} is indeed a generator of the group of points defined over K.

5.12 The curve $\mathcal{E}_{12}$ at (35)

¿From the table of Kodaira reductions, we have $\mu_\nu = 0$ except for

$$\boxed{\mu_\pi = \tfrac{1}{4}, \qquad \mu_{\infty_1} = \mu_{\infty_2} = \mu_{\infty_3} = \tfrac{1}{3}.}$$

Further,

$$\epsilon_\nu^{-1} = \inf_{(X,Y)\in E(K_\nu)} \frac{\max(|f(X)|_\nu, |g(X)|_\nu)}{\max(1,|X|_\nu)^4}$$

with

$$\begin{aligned} f(X) &= 4X^3 + (-12 - 12\phi - 2\phi^2 - 2\phi^3)X^2 + (20 + 24\phi + 6\phi^2 + 4\phi^3)X, \\ g(X) &= (X^2 - (5 + 6\phi + \frac{3}{2}\phi^2 + \phi^3))^2. \end{aligned}$$

Siksek gives a method for computing the ϵ_ν. For the non-Archimedean valuation, we have the following (in Siksek's notation).

First, we observe that $g(1 + \frac{1}{2}\phi + \frac{1}{4}\phi^3) \equiv 0 \pmod{\pi^{10}}$, and $g(X) \not\equiv 0 \pmod{\pi^{12}}$ for any $X \in K$. Thus $\epsilon_\pi = |\pi|_\pi^{-2j} = (2^{-\frac{1}{4}})^{-2j}$, where $j \le 5$. This weak inequality is all that we need, resulting in

$$\boxed{\epsilon_\pi \le 2^{\frac{5}{2}}}.$$

At ∞_1,

$$\epsilon_{\infty_1}^{-1} = \inf_{(X,Y)\in E(\mathbf{R})} \frac{\max(|f(X)|, |g(X)|)}{\max(1,|X|)^4},$$

and the infimum needs to be taken over $X \in \mathbf{R}$ such that $f(X) \ge 0$, that is, over $[0,\infty)$. This infimum occurs at the turning point 4.250162195138054... of $f(X)/X^4$, and has value 0.14604193738214317332..., so that

$$\boxed{\epsilon_{\infty_1} = 6.84734822014400303608...}.$$

At ∞_2,

$$\epsilon_{\infty_2}^{-1} = \inf_{(X,Y)\in E(\mathbf{R})} \frac{\max(|\bar f(X)|, |\bar g(X)|)}{\max(1,|X|)^4},$$

where

$$\begin{aligned} \bar f(X) &= 4X^3 + (-12 + 12\phi - 2\phi^2 + 2\phi^3)X^2 + (20 - 24\phi + 6\phi^2 - 4\phi^3)X, \\ \bar g(X) &= (X^2 - (5 - 6\phi + \frac{3}{2}\phi^2 - \phi^3))^2, \end{aligned}$$

with infimum taken over $X \in \mathbf{R}$ such that $f(X) \ge 0$, that is, over $[0,\infty)$. This infimum occurs at the root 0.007463441518832... of $\bar f(X) - \bar g(X) = 0$, and has value 0.00075564996126157299... so that

$$\boxed{\epsilon_{\infty_2} = 1323.364059108108261943 51...}.$$

At ∞_3,

$$\epsilon_{\infty_3}^{-1} = \inf_{(X,Y)\in E(\mathbf{C})} \frac{\max(|F(X)|, |G(X)|)}{\max(1,|X|)^4},$$

where

$$F(X)^2 = 16X^2(X^4 + (-2+\phi^2)X^3 - 3\phi^2X^2 - 4X + (10+2\phi^2)),$$
$$G(X) = X^4 + (2+3\phi^2)X^2 + (10+2\phi^2).$$

The infimum occurs at the root $-0.309564888209587...-5.048223442072423...i$ of $|F(z)| = |G(z)|$, with value 0.84342888812084072475... (on the unit circle, the minimum taken exceeds 10). Thus

$$\boxed{\epsilon_{\infty_3} = 1.18563641118340119834...}$$

Putting the above together results in

$$\begin{aligned} h(P) - 2\hat{h}(P) \quad \leq \quad & \frac{1}{4}(\frac{1}{4}\cdot 4\cdot \log 2^{\frac{5}{2}} + \frac{1}{3}\cdot 1\cdot \log(6.84734822014400303608) \\ & + \frac{1}{3}\cdot 1\cdot \log(1323.364059108108261943 51) \\ & + \frac{1}{3}\cdot 2\cdot \log(1.18563641118340119834)), \end{aligned}$$

that is,

$$h(P) - 2\hat{h}(P) \leq 1.220913082178307...$$

Suppose now the point G_{12} at (36) is not a generator. We easily check that G_{12} is not divisible by 2 in $E(K)$, and so $G_{12} = mQ$ for $m \geq 3$ and $Q \in E(K)$, with $x(Q) \in \mathcal{O}_K$. Then

$$h(Q) \leq 1.220913082178307 + 2\hat{h}(Q) < 1.220913082178307 + 2\hat{h}(G_{12})/m^2 < 1.234753$$

so that

$$H(Q) < 3.43753.$$

Arguing as in the case of the curve (18), we must consider polynomials of the following types, where $a_i \in \mathbb{Z}$:

$$\begin{aligned} x^4 + 4a_1x^3 + 2a_2x^2 + 4a_3x + a_4, \quad & |a_1| \leq 3, |a_2| \leq 35, |a_3| \leq 40, |a_4| \leq 139, \\ x^2 + 2a_1x + a_2, \quad & |a_1| \leq 3, |a_2| \leq 11, \\ x + a_1, \quad & |a_1| \leq 3. \end{aligned}$$

Each polynomial has to be tested to see if a root can be the X-coordinate of a point in $\mathcal{E}_{12}(K)$. Computation shows that in the given range, only the points $\pm G_{12}$, $\pm G_{12} + (0,0)$, $\pm 2G_{12} + (0,0)$ arise. It follows that G_{12} is indeed a generator of the group of points defined over K.